ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS DE RIESGOS AL PROCESO DE FISCALIZACIÓN DE PROYECTOS DE INGENIERÍA PARA UNA EMPRESA QUE BRINDA SERVICIOS DE INGENIERÍA BAJO LA NORMA ISO/IEC 27005"

TRABAJO DE TITULACIÓN

Previo a la obtención del título de:

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Autores:

CASTILLO PALMA MAPY ASUNCIÓN

MOLINA JIMÉNEZ JOHANNEX KINGSIÑO

Guayaquil – Ecuador

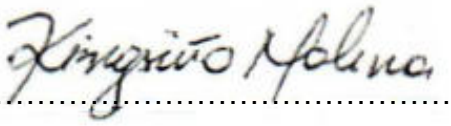
2020

AGRADECIMIENTO

Agradecemos principalmente a Dios por habernos dado valor para continuar cada vez que nos creíamos vencidos. Expresamos nuestro agradecimiento a todas las personas que ayudaron de forma directa e indirecta en la realización de este trabajo de titulación.

……..

Mapy Asunción Castillo Palma



……

Johannex Kingsiño Molina Jiménez

DEDICATORIA

Dedicamos este trabajo de titulación a Dios, creador de todas las cosas, por darnos vida y permitirnos llegar a este momento.

Este trabajo también va dedicado a nosotros mismos por la constancia, por haberlo conseguido, ¡por culminar!

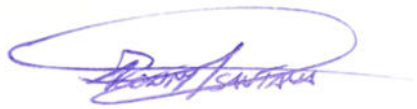
TRIBUNAL DE SUSTENTACIÓN

Msig. Lenin Freire C.

DIRECTOR MSIG

Msig. Lenin Freire C.

DIRECTOR DEL TRABAJO DE TITULACIÓN



Msig. Ronny Santana

MIEMBRO DEL TRIBUNAL

RESUMEN

La Empresa JK Ingeniera es una entidad dedicada a brindar servicios de Ingeniería en proyectos desde su etapa más temprana hasta su desarrollo e implementación, entre los servicios ofertados se encuentra la Fiscalización y Supervisión de Proyectos. En la fase de Ingeniería de Detalle de un Proyecto se genera información y documentación exclusiva de conocimiento entre las partes involucradas por ser la parte creativa de un proyecto. Mantener la privacidad de aquella información en base a su exposición y manipulación resulta un tema prioritario para los directivos de la Empresa.

A pesar de no haber experimentado anteriormente incidentes de seguridad que comprometan las propiedades de la información, se propone implementar la Gestión de Riesgos siguiendo la guía general de la norma ISO 27005, aplicado al proceso de Fiscalización en la etapa de Ingeniería de Detalle que servirá para identificar y disminuir riesgos, así como también representará el punto de partida para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), el tratamiento de los riesgos llevará a la mejora del proceso y sus actividades.

Mientras más valiosa es la información, más controles deben ser aplicados, por ello se ha realizado un análisis de riesgos por cada activo de información identificado en el proceso de Fiscalización; producto de la valoración de riesgos se han seleccionado controles para aquellos riesgos que están fuera del nivel aceptable identificando la causa raíz del problema. Finalmente se elabora un Plan de Tratamiento de Riesgos que contiene el plan de acción para la implementación de los controles ordenado en función al impacto que tendrán los controles sobre el proceso y la organización. La implementación del Plan de Tratamiento de Riesgos permitirá la reducción de los riesgos a niveles aceptables.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

C → Confidencialidad.

COBIT → Control Objectives for Information and related Technology.

D → Disponibilidad.

EO → Estructura Organizacional.

HW → Hardware.

I → Integridad.

IE → Información Electrónica.

IEC → Comisión Electrotécnica Internacional.

II → Información Impresa.

IR → Infraestructura de Red.

ISACA → Information Systems Audit and Control Association.

ISF → Information Security Forum.

ISO → Organización Internacional de Normalización.

ITGI → IT Governance Institute.

MAGERIT → Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

NIST → National Institute of Standards and Technology.

OCTAVE → Operationally Critical Threat Asset and Vulnerability Evaluation.

P → Proceso.

PER → Personal.

PHVA → Planear, Hacer, Verificar, Actuar.

R-C → Riesgo en Confidencialidad.

R-D	→	Riesgo en Disponibilidad.
R-I	→	Riesgo en Integridad.
S	→	Sitio.
SGSI	→	Sistema de Gestión de Seguridad de la Información.
SW	→	Software.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Actualmente en todo tipo de empresas existe un interés creciente en invertir parte de sus recursos en proporcionar seguridad a los activos que posee la organización, uno de estos activos es la información. La información aun siendo en ocasiones un activo intangible puede ser víctima de incidentes de seguridad impactando la operación de una empresa en diferentes grados de acuerdo a su criticidad.

Los riesgos propios de las actividades de una empresa por la manipulación de sus activos deben ser analizados para derivar en controles que mitiguen la causa raíz del inherente peligro de impacto, ya que cada empresa y cada activo varía en funciones, este análisis debe ser particular de acuerdo a la realidad de la organización y sus procesos.

La empresa JK Ingeniería, debido a que su mayor activo es la información, se ha visto interesada en darle un grado más de confiabilidad a los servicios que entrega anticipándose ante una eventual alteración en su seguridad. Se ha solicitado la intervención de uno de sus procesos y se evaluarán las consecuencias de la pérdida de confidencialidad, integridad y disponibilidad de

los activos aplicando la metodología de Gestión de Riesgos proporcionada por la Norma ISO 27005 que permite identificar, analizar y valorar los efectos de los riesgos y las acciones correctivas para los mismos en base al contexto de la organización.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

"JK – Ingeniería" es una empresa local dedicada a brindar servicios de Desarrollo, Implementación y Consultoría de proyectos de Ingeniería tanto Mecánica, Eléctrica, Electrónica y de Redes de Datos para clientes de los cuales destacan: restaurantes, hoteles, centros hospitalarios, urbanizaciones, Municipios, entre otros; quienes solicitan uno o varios de los servicios del catálogo vigente.

Dentro de los servicios categorizados como Consultoría, la empresa JK ofrece el servicio de Fiscalización de Proyectos, en el cual la empresa actúa como un ente intermedio entre el Cliente y la empresa gestora del

proyecto, brindándole acompañamiento y seguimiento desde el levantamiento de requerimientos, diseño, construcción e implementación de este, teniendo desde el inicio libre acceso a todos los datos e información concernientes a cada una de las etapas del proyecto. Un proyecto de Ingeniería consta de las siguientes etapas o fases:

1. Ingeniería de Perfil o Prefactibilidad.
2. Ingeniería Conceptual.
3. Ingeniería Básica o de Factibilidad.
4. Ingeniería de Detalle.
5. Ingeniería Constructiva.
6. Ingeniería de Operación.

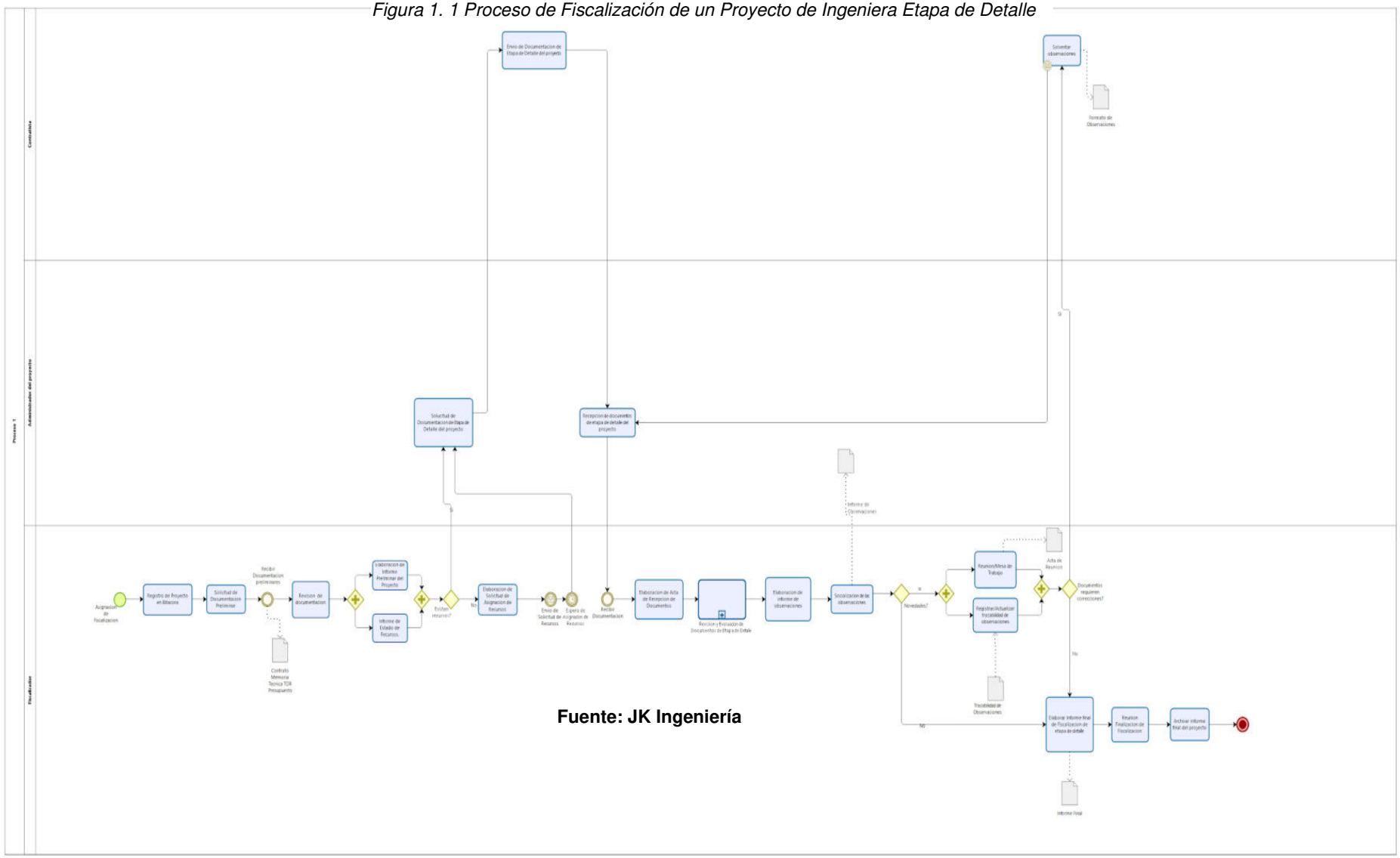
Según haya sido el contrato, la Empresa realiza la asistencia técnica y gestión documental necesaria para llevar a cabo la Fiscalización de una o varias etapas dentro del proyecto.

1.2 DESCRIPCIÓN DEL PROBLEMA

La etapa que más entradas y salidas de información genera dentro del proceso de Fiscalización es la etapa de Ingeniería de Detalle (Figura 1.1), la cual analiza de forma particular los documentos emitidos por el gestor del proyecto para esta etapa y los compara con los documentos resultantes de las etapas anteriores antes de entrar a la etapa constructiva con el fin de evaluar si se cumplen de forma técnica y

económica con los objetivos y métricas propuestas en la etapa de concepción del proyecto. Este análisis arroja un conjunto de documentos técnicos e informativos necesarios para la aprobación de ejecución del proyecto.

Figura 1. 1 Proceso de Fiscalización de un Proyecto de Ingeniera Etapa de Detalle



Fuente: JK Ingeniería

Siendo los datos y la información los activos más valiosos y relevantes para las organizaciones de los clientes, resulta vital el poder brindar control y protección de manera adecuada frente a las posibles vulnerabilidades y amenazas existentes dentro del proceso.

Hasta el momento, la Empresa no ha experimentado consecuencias provocadas por una brecha de seguridad generada por sus activos o por su personal, sin embargo, el diagnóstico permitirá en un futuro el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado a la norma ISO / IEC 27001.

La posible presencia de un incidente de Seguridad podría afectar la reputación de la Empresa, haciendo disminuir la confianza del cliente hacia los Ingenieros que brindan servicios, paulatinamente esto podría incidir en los ingresos que se perciben traduciéndose en perdidas significantes de dinero.

1.3 SOLUCIÓN PROPUESTA

Se propone determinar el valor de los activos identificando amenazas y vulnerabilidades, con lo que se pueda obtener una Matriz de Riesgo valorada siguiendo las normativas de diagnóstico que establezcan el estado actual de seguridad del proceso de Fiscalización.

Lo mencionado garantizará la identificación de las causas de las vulnerabilidades encontradas, permitiendo proponer soluciones de control y mitigación con el propósito de lograr el ambiente adecuado para el

correcto manejo de información de clientes, manteniendo la confidencialidad, integridad, disponibilidad y autenticidad de la misma.

La normativa a seguir es la ISO / IEC 27005 que provee los lineamientos que indican qué es lo que se requiere para la gestión del riesgo.

1.4 OBJETIVO GENERAL

Realizar el análisis de riesgo de los activos del proceso de Fiscalización de proyectos en una empresa que brinda servicios de Ingeniería.

1.5 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información del proceso de Fiscalización de proyectos.
- Evaluar los activos de información en función de la confidencialidad, integridad y disponibilidad.
- Realizar el análisis para definir la Matriz de Riesgo en función de las amenazas al proceso definido.
- Elaborar un plan de tratamiento del riesgo para su implementación a corto plazo.

1.6 METODOLOGÍA

Para llegar al objetivo principal del presente trabajo, se evaluará el estado actual de los activos de información del proceso de Fiscalización de la Etapa de Detalle de un proyecto de Ingeniería, de esta evaluación se identificarán los incidentes de seguridad encontrados. Se deberá identificar cada aspecto

relevante que deba ser considerado dentro del trabajo para determinar el alcance del mismo.

Se determinarán las vulnerabilidades y amenazas del proceso mediante el análisis de brecha que permitirá estimar e identificar los riesgos respecto a los criterios de información: confidencialidad, integridad y disponibilidad. Una vez se hayan evaluado dichos análisis se determinarán las estrategias para responder ante los riesgos y los controles de seguridad aplicables que servirán de base para elaborar propuestas de proyectos que ayuden a frenar las brechas de seguridad encontradas.

La metodología propuesta está basada en la valoración de riesgos del estándar ISO/IEC 27005.

CAPÍTULO 2

MARCO TEÓRICO

2.1 NORMATIVAS DE LA SEGURIDAD DE LA INFORMACIÓN.

Las normativas de Seguridad de la Información tienen como objetivo asegurar y regularizar el acceso a la misma. En Ecuador, la Constitución de la República, vigente desde el año 2008 dice en su Artículo 66 numeral 19 que "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley." [1]

Para asegurar este derecho, la Constitución incluye el Habeas Data en su artículo 92 en el que dice que "Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino personal y el tiempo de vigencia del archivo o banco de datos."

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional indica que se interpondrá el habeas data cuando: se niegue acceso a documentación o datos personales que consten en entidades públicas, cuando se niegue la actualización o anulación de datos erróneos, o cuando se use información personal que viole alguno de los derechos constitucionales, sin autorización expresa o sin autorización de un juez. [2]

Ecuador también ha adoptado las Normas Técnicas de Seguridad de la familia de estándares internacionales ISO/IEC 27000, estas normas consisten de varios estándares para seguridad de información el cual fue desarrollado por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission), se basa en la elaboración dentro de una organización de un SGSI (Sistema de Gestión de Seguridad de la Información), se tiende a pensar que este grupo de normas sólo es aplicable a organizaciones desarrolladoras de Software, sin embargo esto no es limitante ya que puede ser

aplicado a cualquier tipo de organización que desenvuelva en otros tipos de mercado [3]. Esta familia de normas será descrita en la sección 2.2

Uno de los marcos de referencia definido para gobernanza y administración de empresas TI es el COBIT (Control Objectives for Information and related Technology) cuya versión actual es la 5, fue desarrollado por ISACA (Information Systems Audit and Control Association) y el ITGI (IT Governance Institute). Este framework está basado en principios, prácticas, herramientas de análisis y modelos globalmente aceptados que permiten a los gerentes y administradores, comprender el nivel de seguridad y control que necesitan para proteger los activos de sus empresas [4]. De COBIT v4.1 y el estándar ISO/IEC 27002 se deriva el Estándar de Buenas Prácticas para Seguridad de la Información, fue publicado por primera vez en 1996 y su última actualización fue en el año 2018, este grupo de buenas prácticas fue creado por Chaplin y Creasey y publicado por el ISF (Information Security Forum). Este provee ideas de una metodología funcional para seguridad de la información basada tanto en la investigación como en la experiencia de la vida real [5].

2.2 FAMILIA DE NORMAS ISO 27000

La familia ISO/IEC 27000 está compuesta de más de 50 documentos de directrices y estándares interrelacionados, los cuales muchos ya han sido publicados y otros se encuentran aún en desarrollo. Esta familia de normas es creada por una amplia variedad de organizaciones y compilado por la ISO.

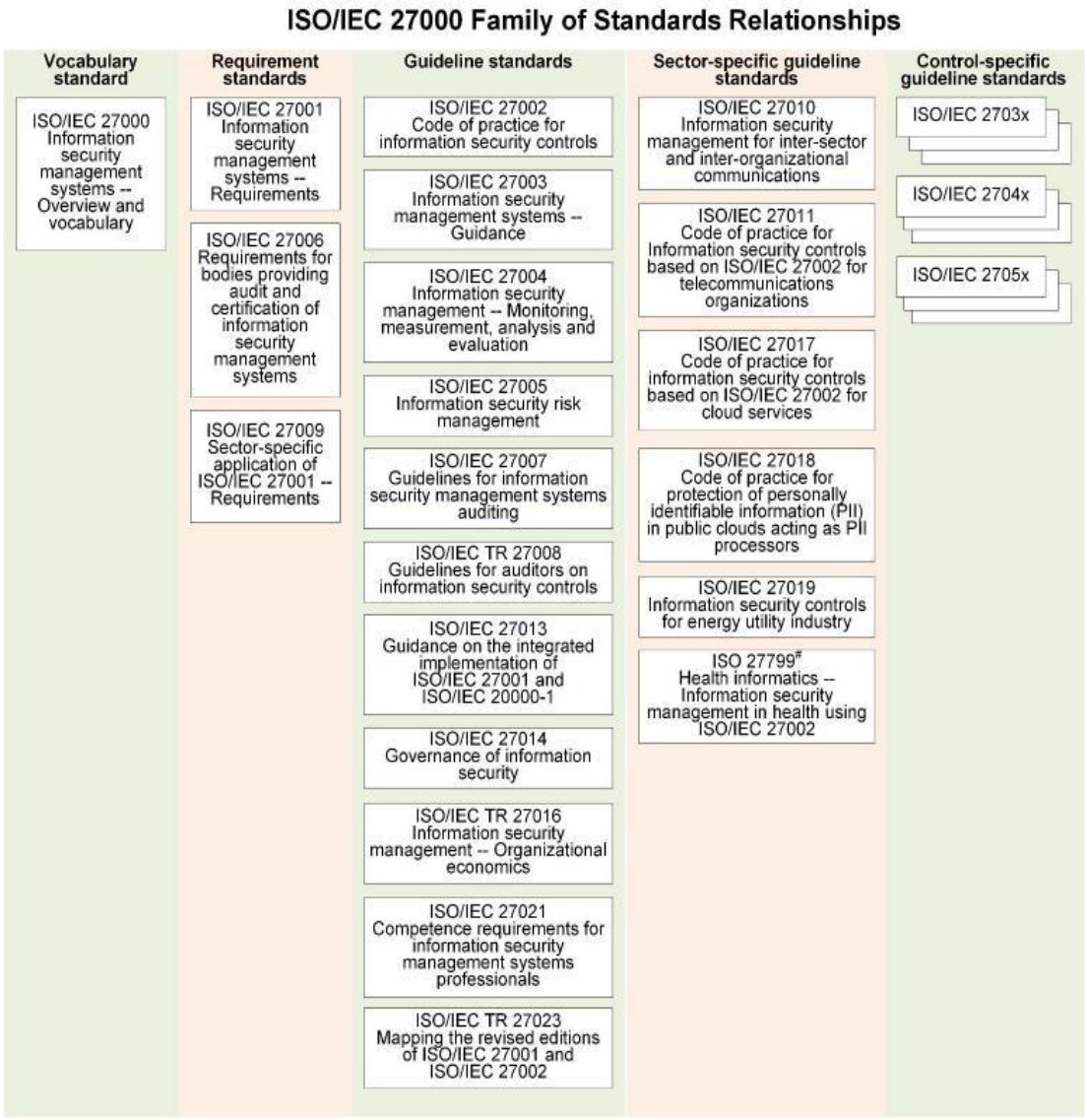
Las normas ISO/IEC 27000 proporcionan recomendaciones de mejores prácticas en Gestión de Seguridad de la Información, Gestión de Riesgo y Controles de

Seguridad dentro del contexto de un SGSI general; las normas también se enfocan en describir los requisitos del SGSI (ISO/IEC 27001) y los requisitos del organismo de certificación (ISO/IEC 27006), otras normas proveen orientación para varios aspectos de implementación del SGSI para que una organización cree y diseñe su SGSI que se adapte a su propio propósito comercial. Cualquier tipo de organización, como parte integral de su plan de negocios, podría encontrar en la Seguridad de la Información un método para mejorar la rentabilidad de la misma. [3]

Las normas ISO/IEC 27000 guían la implementación del SGSI basándose en los objetivos estratégicos de gestión y gobernanza, esos objetivos iniciales se describen como: la Política de Seguridad de la Información, la Política de Gestión de Riesgos y las definiciones de seguridad de la organización. La arquitectura de seguridad de la información será definida para los activos en los documentos mencionados anteriormente. El requisito básico para un SGSI funcional es que exista un proceso de evaluación de seguridad de la información predefinido, el cual deberá revelar si existen posibles brechas en la actividad y establecerá nuevos objetivos para el desarrollo del SGSI. [6]

En la gráfica a continuación se muestra la relación entre las normas de la familia ISO/IEC 27000, las normas se aplican para: describir una visión general y definir terminología, especificar requisitos, definir lineamientos generales y describir directrices específicas del sector.

Figura 2. 1 Familia de Estándares ISO/IEC 27000



Fuente: Office of the Government Chief Information Officer

A continuación, se describe brevemente lo más destacado de la familia de normas ISO/IEC 27000 desde el punto de vista de Seguridad de la Información [3]:

- **ISO/IEC 27001: 2013.** Esta norma establece los requerimientos para la definición, implementación, operación, supervisión, mantenimiento y mejora de un SGSI.
- **ISO/IEC 27002: 2013.** Código de prácticas para la gestión de la seguridad de la información. Guía de implementación de controles, establece las directrices para comenzar, implementar, mantener y mejorar la gestión de la Seguridad de la Información de la organización.
- **ISO/IEC 27005: 2018.** Gestión de Riesgos de Seguridad de la Información. Brinda soporte a la ISO/IEC 27001

Parte de las normas ISO/IEC 27000 cubre otras áreas fuera del alcance de seguridad de la información, como la 27032: Gestión de la Ciberseguridad, 27033: Seguridad en la red, 27034: Seguridad de Aplicaciones, 27037: Norma para la identificación, recopilación, adquisición y preservación de evidencia digital [3].

Los principales beneficios de aplicar las normas ISO/IEC 27000 son las siguientes:

- Competitividad.
- Conformidad.
- Rentabilidad.
- Imagen.

2.3 METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS

La necesidad de precautelar los activos de información y proteger sus propiedades (disponibilidad, confidencialidad e integridad) ha llevado consigo la

evolución de la Seguridad de la Información y Gestión de Riesgos. Para cumplir con la necesidad de prevenir riesgos dentro de las organizaciones, los organismos internacionales han desarrollado estándares / normas para la Seguridad de la Información tales como la ya descrita familia de normas ISO/IEC 27000, metodologías en relación a la Gestión de Riesgos como la ISO 31000, ISO 27005, MAGERIT, OCTAVE, NIST 800-30, CRAMM, entre otras.

ISO 31000. Familia de normas que abarca pautas y directrices genéricas para las buenas prácticas de la Gestión de Riesgos proporcionando un paradigma universalmente reconocido. Codificada y publicada como estándar el 13 de noviembre de 2009 por la ISO, tiene como objetivo ayudar a las organizaciones a gestionar el riesgo con efectividad sin importar el tamaño o el tipo de la organización. Establece una serie de principios básicos que deben cumplirse para gestionar el riesgo de cualquier tipo, tanto en consecuencias positivas como negativas, recomendando que las organizaciones desarrollen, ejecuten y mejoren continuamente su framework [8].

Los principios básicos que debe cumplir una organización son:

- Crear valor.
- Estar integrada a los procesos de la organización.
- Estar presente en el proceso de toma de decisiones.
- Tratar explícitamente la incertidumbre.
- Ser sistemática, estructurada y adecuada.
- Se basa en la mejor información disponible.
- Se adapta a circunstancias locales y específicas.

- Toma en cuenta factores humanos y culturales.
- Es transparente e inclusiva.
- Sensible al cambio.
- Facilita la mejora continua de la organización.

El proceso de la ISO 31000 es caracterizado por la identificación, análisis, evaluación, tratamiento, comunicación y seguimiento del riesgo que está afectando a la organización sin importar su tipo.

La familia ISO 31000 incluye: ISO 31000:2009 - Principios y Directrices para la implantación, ISO/IEC 31010:2009 - Gestión del riesgo - Técnicas de evaluación de riesgos, Guía ISO 73:2009 - Gestión del riesgo - Vocabulario.

ISO 27005. Esta norma proporciona las directrices para la gestión de riesgos en la seguridad de la información de una organización, apoyando los requisitos generales del SGSI definidos en la ISO 27001 y 27002 el conocimiento de los conceptos, modelos, procesos y términos descritos en estas normas es complemento necesario para el entendimiento de la norma ISO 27005; fue diseñada para aplicar de forma satisfactoria la seguridad de la información con enfoque en gestión de riesgos. Es aplicable a cualquier tipo de organización donde se pretenda gestionar los riesgos como empresas comerciales, entes gubernamentales u organizaciones sin fines de lucro. Esta norma no proporciona o recomienda una metodología específica, aquello depende de factores como el alcance del SGSI, tamaño o sector productivo de la organización [9].

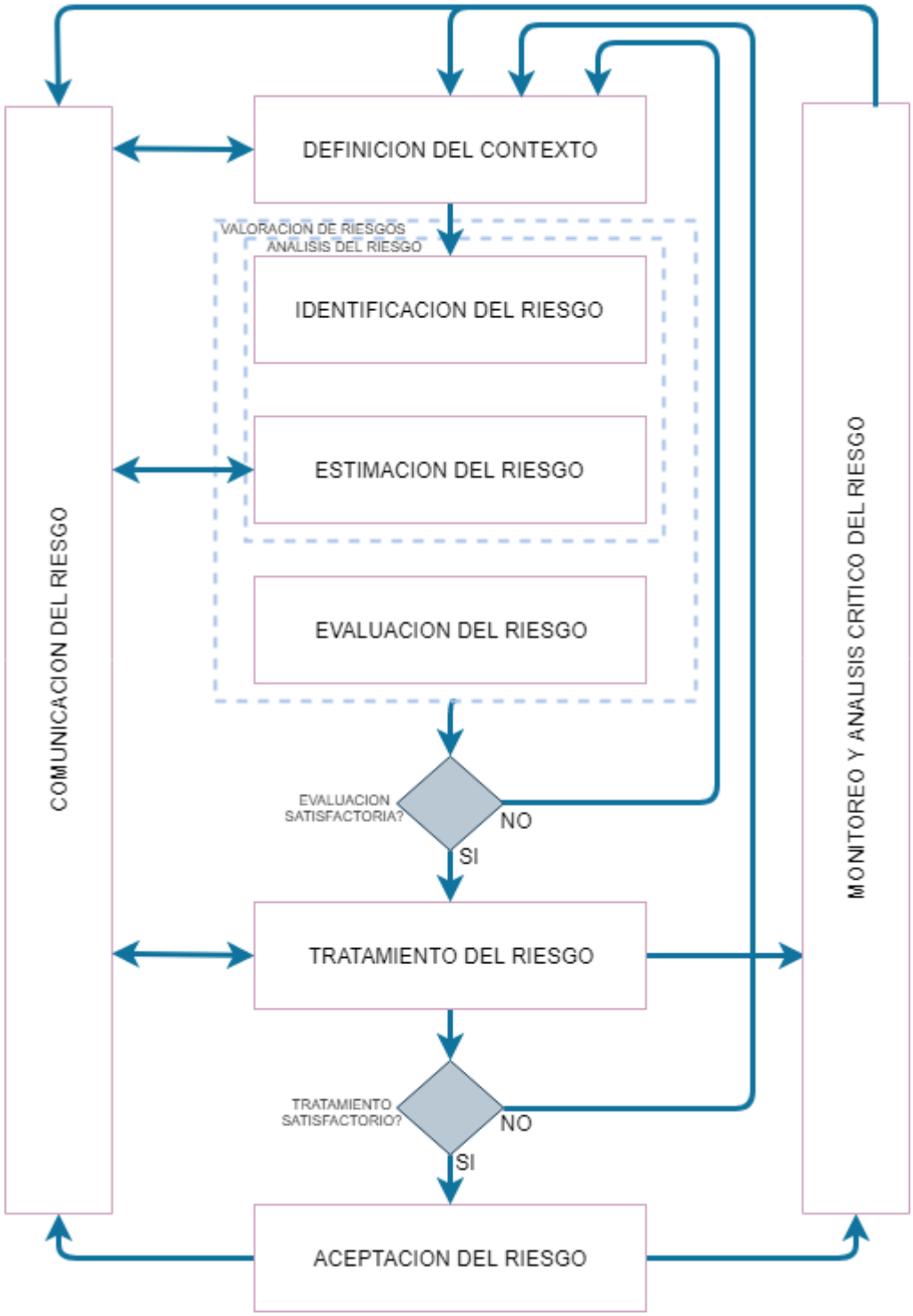
La primera versión fue publicada el 4 de junio de 2008, la última versión fue publicada en 2018. La gestión del riesgo puede ser aplicable a toda la

organización, una porción de ella, a una parte separada de la misma, a cualquier sistema de información existente o planificado, a su vez puede ser aplicado a aspectos particulares de control [3].

El proceso para la gestión de riesgos puede ser iterativo para las actividades de valoración y tratamiento de riesgos. Se conoce primero el contexto, luego se valora el riesgo, para continuar con el tratamiento del riesgo se debe proporcionar la información suficiente que ayuden a determinar las acciones que se necesitan para mitigar los riesgos. Si la información no es suficiente se revisa el contexto nuevamente. La correcta aplicación del tratamiento del riesgo depende de resultados adecuados en la valoración del riesgo. Es posible que inicialmente el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual [9].

La estructura de la norma está definida por:

Figura 2. 2 Proceso de Gestión de Riesgo



Fuente: ISO/IEC 27005:2018

La ISO 27005 se definió para riesgos informáticos y se encuentra alineada a la ISO 31000 y como otras normas ISO tiene como metodología de implementación y mejora continua al ciclo PHVA (Planear-Hacer-Verificar-Actuar) aplicado a la Gestión de Riesgo de la Seguridad de la Información [10]. A continuación, se presenta la alineación entre el ciclo de Deming PHVA y la ISO 27005:

Tabla 1 Alineación Ciclo de Deming PHVA - ISO 27005

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th></tr>
<tr><td rowspan="8">PLANEAR</td><td colspan="2">Definir plan de gestión de riesgos</td><td rowspan="10">Proceso de gestión del riesgo.</td></tr>
<tr><td colspan="2">Definición del contexto.</td></tr>
<tr><td>Identificación del riesgo.</td><td rowspan="3">Valoración del riesgo.</td></tr>
<tr><td>Estimación del riesgo.</td></tr>
<tr><td>Evaluación del riesgo.</td></tr>
<tr><td colspan="2">Plan de tratamiento del riesgo.</td></tr>
<tr><td colspan="2">Aceptación del riesgo.</td></tr>
<tr><td rowspan="2">HACER</td><td colspan="2">Implementar el plan de tratamiento.</td></tr>
<tr><td colspan="2">Implementar plan de comunicación de riesgo.</td></tr>
<tr><td>VERIFICAR</td><td colspan="2">Monitoreo y revisión del riesgo.</td></tr>
<tr><td>ACTUAR</td><td colspan="2">Mantener y mejorar el proceso de gestión.</td></tr>
</table>

Fuente: A. Ramírez & Z. Ortiz

Según la norma, la gestión de riesgos debería contribuir a [9]:

- Identificación del riesgo.
- Evaluación del riesgo en términos de consecuencias para el negocio y su probabilidad de ocurrencia.
- Establecer un orden de prioridades para el tratamiento del riesgo.
- La priorización de las acciones para la disminución de la ocurrencia.

- Participación e involucramiento de los interesados cuando se toman las decisiones sobre la gestión del riesgo.
- La eficacia del monitoreo del tratamiento del riesgo.
- Educación sobre el riesgo y las acciones que se toman para mitigarlo.

MAGERIT. Esta metodología de análisis y gestión de riesgos fue desarrollada por el Consejo Superior de Administración Electrónica en España como respuesta a la creciente dependencia de la Tecnología en la sociedad para el cumplimiento de sus objetivos. Presenta una guía completa y paso a paso de cómo llevar a cabo un análisis de riesgo; consta de tres volúmenes: Método, Catálogo de Elementos para aplicar la metodología y Guía de Técnicas y ejemplos a usar en los diferentes pasajes de la Gestión de Riesgos [11].

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de información, que supone beneficios para los usuarios, pero también da lugar a riesgos que deben ser minimizados con medidas de seguridad que generen confianza. MAGERIT actualmente está en su versión 3.

Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de información y comunicaciones para de esta forma implementar las medidas más adecuadas que permitan mantener los riesgos mitigados. Si la información resultante o los servicios que se prestan gracias a ella son importantes, MAGERIT permite saber cuánto valor esta

información/servicio representa y así ayudar a protegerlos identificando amenazas y vulnerabilidades que puedan afectar a la organización. Conocer el riesgo y el impacto que genera la violación de seguridad de los elementos de trabajo es indispensable para saber cómo gestionarlos e identificar claramente medidas preventivas y correctivas apropiadas [11].

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación ni dependa de la arbitrariedad del analista.

MAGERIT persigue los siguientes objetivos directos [11]:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar tales riesgos.
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Objetivos indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

OCTAVE: Los métodos OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation) es un enfoque usado para evaluar las necesidades de seguridad de la información de una organización y propone un plan de mitigación de los mismos. Los métodos OCTAVE son autodirigidos, flexibles y evolucionados. Equilibran aspectos de riesgos operativos, prácticas de seguridad

y tecnología para que, a partir de estos, los directivos de la organización puedan tomar las decisiones correctas en temas de protección de la información basados en los principios de seguridad [12].

El uso de OCTAVE permite que equipos pequeños, a través de unidades de negocios, y el TI trabajen juntos para abordar los requisitos de seguridad de la organización, por lo que además buscan dar a conocer la importancia de que cada uno de los miembros de la organización conozca sobre el valor de sus activos y los riesgos que amenazan su entorno de actividad. Son métodos adaptables al entorno de riesgo de la organización, a sus objetivos de seguridad, resiliencia y nivel de habilidad.

Tiene tres métodos que son [13]:

1. Octave método original: Se aplica a organizaciones de 300 o más empleados, pero también se debe de tener en cuenta la jerarquía de la organización.
2. Octave-S: Enfocada a las empresas pequeñas.
3. Octave-Allegro: Una opción para evaluar riesgos de seguridad en 8 pasos.

Esta metodología se enfoca en las actividades diarias de la organización, partiendo de la identificación y valoración de los activos de información, como cualquier otro método para este fin.

NIST 800-30: Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), concebido para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI, proporciona una guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica. También provee fundamentos para la administración de riesgos, así como la evaluación y mitigación de los riesgos identificados dentro del sistema de TI con el objetivo de apoyar a las organizaciones con todo lo relacionado a tecnología [13].

Esta metodología se estructura de la siguiente manera:

- Proceso de Análisis de Riesgos, consta de 9 pasos [13]:
    1. Caracterización del sistema: permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa.
    2. Identificación de amenazas: donde se definen las fuentes de motivación de las mismas.
    3. Identificación de vulnerabilidades: En esta fase desarrolla una lista de defectos o debilidades del sistema que podrían ser explotadas por una amenaza
    4. Análisis de controles: Lista de controles actuales
    5. Determinación de probabilidades: Ayuda a evaluar el rango de probabilidad de que una vulnerabilidad se convierta en amenaza.
    6. Análisis del impacto: Analizarán el impacto que puedan repercutir los riesgos

7. Determinación del riesgo: Ayuda a evaluar el riesgo en el sistema de información
8. Recomendaciones de control: En donde se proporcionan los controles que podrían mitigar el riesgo identificado o llevándolo a un nivel aceptable
9. Documentación de resultados: se genera un informe con la descripción de las amenazas y vulnerabilidades, midiendo el riesgo y generando recomendaciones para la implementación de los controles.

- Fase de gestión de riesgos, consta de 7 pasos [14]:
  1. Priorización de acciones.
  2. Evaluación de opciones de controles recomendados.
  3. Análisis de coste-beneficio.
  4. Selección de controles que ayudarían a eliminar riesgos.
  5. Asignación de responsabilidades.
  6. Desarrollo del plan de implantación.
  7. Implantación de controles seleccionados.

2.4 GESTIÓN DE RIESGO COMO BASE DE UN SGSI

La gestión del riesgo implica inversión de tiempo, esfuerzo y otros recursos con los que una pequeña organización no suele disponer, siendo esta una de las razones por las que no suelen considerar la gestión del riesgo como una prioridad.

Según el físico y matemático británico William Thomson Kelvin, *"Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre."* La medición es imprescindible en la Gestión, en una organización medir el impacto del riesgo aporta a un mejor entendimiento de criterios de disponibilidad, integridad y confidencialidad de la información.

La información es un activo de valor vital para el éxito y prolongación en el mercado de cualquier organización [15]. Todas las organizaciones se enfrentan a factores internos y externos que generan incertidumbre sobre si serán víctimas de las consecuencias de un fallo en la Seguridad de la Información, el efecto de esta incertidumbre es el riesgo y es por esto que debe ser controlado y gestionado con el objetivo de llevarlo a niveles asumibles para la organización [16].

La seguridad absoluta no existe por lo que la forma de conseguir un mayor beneficio de la Seguridad de la Información, es contar con una correcta evaluación y medición del riesgo en los diferentes niveles de la organización. Una evaluación del riesgo exhaustiva y adecuada tiene como resultado la reducción de pérdidas, robo o corrupción de la información. La gestión del riesgo evaluará el daño resultante de una falla y la probabilidad de ocurrencia, estimará el nivel de riesgo resultante y determinará si el riesgo es aceptable o requiere de un tratamiento [17].

CAPÍTULO 3

IDENTIFICACIÓN Y EVALUACIÓN DE LOS ACTIVOS DE INFORMACIÓN

3.1 DEFINICIÓN DEL CONTEXTO DE LA ORGANIZACIÓN.

Para comenzar el proceso de Gestión de Riesgos, lo primero a realizar según la norma ISO 27005 es el levantamiento de toda la información concerniente a la organización donde sería ejecutado el análisis de riesgo [9].

3.1.1 DETERMINACIÓN DEL ALCANCE

VISIÓN DE LA EMPRESA:

La empresa JK Ingeniería tiene como visión posicionarse como líder del mercado ecuatoriano en soluciones integrales en diversas áreas de Ingeniería, Seguridad y Tecnología.

MISIÓN DE LA EMPRESA:

Por otra parte, la misión de la empresa es forjar relaciones de confianza con sus clientes, colaboradores, proveedores y contratistas a través de personal altamente calificado que responda ante las situaciones presentadas, entregando soluciones especializadas en ámbitos de Desarrollo, Implementación y Consultoría de proyectos de Ingeniería, tanto Mecánica, Eléctrica, Electrónica y de Tecnología.

OBJETIVOS:

Fortalecer el Desarrollo de Proyectos de Ingeniería proporcionando un equipo de Ingenieros especialistas en cada arista del proyecto para lograr el cumplimento de los objetivos estratégicos del mismo.

Ofrecer consultoría necesaria para el correcto Desarrollo de Proyectos de Ingeniería, optimizando el uso de los recursos.

Impulsar el uso de nuevas tecnologías de Seguridad Electrónica para uso residencial y comercial.

Brindar servicios de Consultoría y Construcción de Sistemas Contra Incendio, basados en normas nacionales e internacionales.

ALCANCE DE LA GESTIÓN DE RIESGOS:

De acuerdo con el ambiente confidencial en el que se brindan los servicios de la Empresa, se plantea el alcance de la Gestión de Riesgos como la evaluación de los procesos críticos que podrían generar mayor impacto en la pérdida de confiabilidad de los servicios ofertados.

La Gestión de Riesgo involucra:

- Todo el personal de la empresa JK Ingeniería.
- Documentación recibida y generada en los procesos críticos.
- Tecnología usada en los procesos críticos.

3.1.2 SELECCIÓN DE PROCESOS CRÍTICOS

Se considera al proceso de Fiscalización de Proyectos de Ingeniería como el más crítico de la empresa, debido a que involucra la manipulación y generación de documentación confidencial que es fundamental para el desarrollo de las actividades propias de los proyectos.

3.1.3 DESCRIPCIÓN DE LOS CRITERIOS DE EVALUACIÓN

Se considera el tipo cualitativo como metodología para estimación del riesgo. Como criterios de evaluación de la probabilidad de ocurrencia de una amenaza, se utiliza la Tabla 2 como escala de atributos calificativos.

Tabla 2 Escala de Atributos Calificativos de Probabilidad

NIVEL	**EQUIVALENCIA CUANTITATIVA**
ALTO	3
MEDIO	2
BAJO	1

Fuente: Los Autores

Para evaluar el impacto de la materialización de una amenaza, es necesario determinar las consecuencias de la pérdida de confidencialidad, integridad y disponibilidad de los activos.

[D] Disponibilidad: Requiere que la información sea accesible para las personas involucradas. ¿Qué pasaría si la información de esos activos no está disponible cuando se lo requiere?

[I] Integridad: Supone que la información se mantenga inalterada ante un evento de seguridad. ¿Qué pasaría si los datos fueran modificados sin autorización o control?

[C] Confidencialidad: Prevenir la divulgación no autorizada de información de la organización. ¿Qué pasaría si esa información es conocida por personas no autorizadas o fuera de la organización?

Se utiliza la Tabla 3 como escala de nivel de impacto de una amenaza al explotar una vulnerabilidad.

Tabla 3 Escala de Nivel de Impacto de una Amenaza

NIVEL	**EQUIVALENCIA CUANTITATIVA**
ALTO	3
MEDIO	2
BAJO	1

Fuente: Los Autores

Se estima como riesgos inaceptables, aquellos riesgos que tengan como resultado 9 y a estos se les debe aplicar controles, los demás riesgos serán

considerados como aceptables. En la Tabla 4 se detalla el resultado de la multiplicación de:

Riesgo = Impacto x Probabilidad

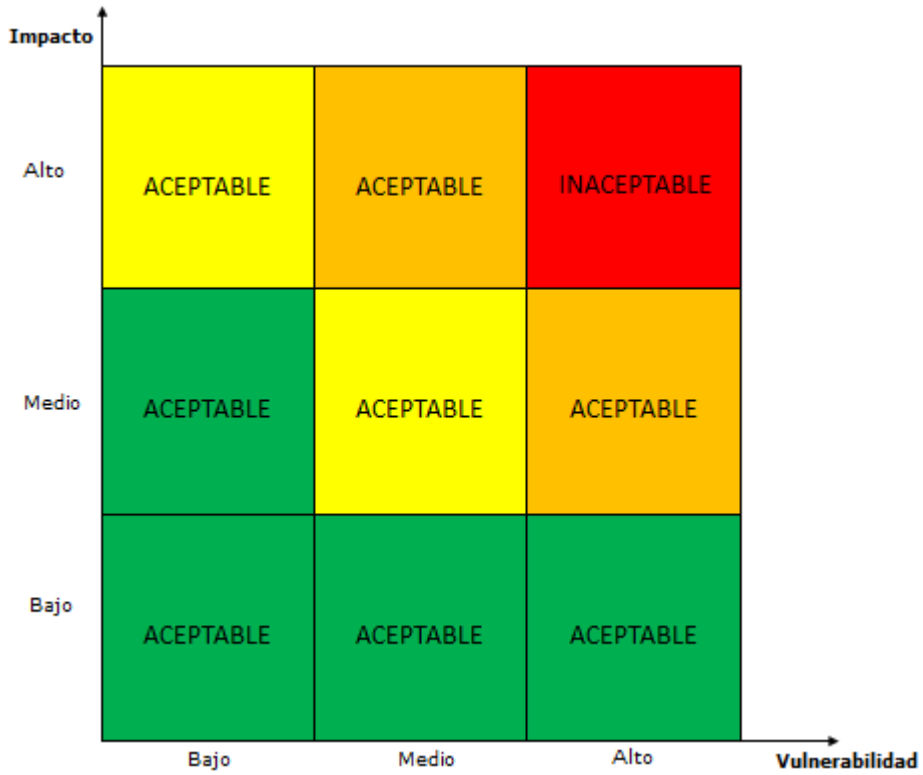
Tabla 4 Impacto x Probabilidad

NIVEL	**IMPACTO**	**AMENAZA/PROBABILIDAD**
INACEPTABLE	ALTO	ALTO
ACEPTABLE	ALTO	MEDIO
	ALTO	BAJO
	MEDIO	ALTO
	MEDIO	MEDIO
	MEDIO	BAJO
	BAJO	ALTO
	BAJO	MEDIO
	BAJO	BAJO

Fuente: Los Autores

Una vez que se ha definido los niveles de aceptabilidad, se los puede representar en un mapa de calor:

Figura 3. 1 Niveles de Aceptabilidad



Fuente: Los Autores

3.2 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Un activo es cualquier elemento crítico que contenga información, que le de valor a la organización y que necesite ser protegido.

Entradas: Determinar la información que es utilizada y generada durante el proceso de Fiscalización de un Proyecto de Ingeniería en su etapa de Diseño.

Los siguientes son los grupos de clasificación de activos:

[P] → Proceso.

[HW] Hardware → Se refiere a la parte física de un dispositivo electrónico.

[SW] Software → Aplicaciones, software o sistemas informáticos.

[IE] Información Electrónica → Conformada por archivos.

[II] Información Impresa → Cualquier registro que no sea tratado digitalmente, será considerado como Información Impresa.

[IR] Infraestructura de Red → Elementos que permiten la intercomunicación entre los dispositivos electrónicos de la red.

[PER] Personal → Personal que forma parte de las actividades diarias de la organización.

[S] Sitio → Edificación en donde se desarrollan las actividades del proceso.

[EO] Estructura Organizativa → Organigrama, roles y funciones.

Al identificar los activos y su clasificación, es necesario también identificar a sus propietarios, quienes son responsables de cada activo.

A continuación, se detalla el Inventario de Activos:

Tabla 5 Inventario de Activos

No.	Nombre del Activo	Tipo de Activo	Tipo	Descripción	Propietario del Activo
1	Orden de Trabajo	IE	Interno	Documento en el cual se expone el tipo y descripción del proyecto y las personas asignadas al mismo	Dpto. Comercial

2	Bitácora de Trabajos	IE	Interno	Documento donde se registran los proyectos en los que se encuentra trabajando el personal, se encuentra guardado y compartido en la Nube.	Dpto. Proyectos
3	Términos de Referencia	II / IE	Externo	Documento que la entidad contratante elabora para exponer los requerimientos que necesita, con el fin de que los contratistas puedan hacer sus ofertas técnicas y económicas	Cliente
4	Contrato de Obra	II	Externo	Documento donde se detallan los derechos y obligaciones del cliente y el contratista en mutuo acuerdo para adquirir un servicio	Cliente
5	Memoria Técnica Preliminar	II	Externo	Documento donde se expresa una clara síntesis del proyecto, como descripción de los datos más importantes de la obra, necesidades, plan de trabajo, estimación y asignación de recursos y presupuesto	Cliente
6	Especificaciones Funcionales	II	Externo	Documentos que definen los lineamientos generales e ideas básicas del proyecto, que serán los pilares de la ingeniería de detalle	Cliente
7	Planos de ubicación	II	Externo	Documentos gráficos y escritos necesarios para la elaboración de la ingeniería de detalle	Cliente

8	Presupuesto referencial	II	Externo	Documento que de manera básica muestra el monto económico para la construcción del proyecto	Cliente
9	Aval de recursos	IE	Interno	Documento donde se evalúan los recursos con los que cuenta el departamento de proyectos y se proponen los que se necesitan para empezar la etapa de fiscalización	Dpto. Proyectos
10	Solicitud de asignación de recursos	IE	Interno	Documento donde se especifica a detalle cada uno de los requerimientos que necesita el departamento de proyectos para completar sus recursos y empezar la fiscalización	Dpto. Proyectos
11	Proceso de Adquisición de Recursos	P	Interno	Proceso donde se detallan las etapas y aprobaciones requeridas para adquirir un bien o servicio	Dpto. Adquisiciones
12	Acta de Recepción	II	Interno	Documento donde se indican los documentos que se reciben de manera escrita por parte de la empresa contratista	Dpto. Proyectos
13	Acta de Inicio de fiscalización	II	Interno	Documento que marca el inicio de la etapa de detalle donde están los compromisos que tiene el contratista en la nueva etapa	Dpto. Proyectos

14	Informe Preliminar del proyecto	II / IE	Interno	Documento realizado por el equipo encargado de la fiscalización donde somete la ingeniería básica a una cuidadosa revisión, detectando las observaciones que merezca y proponiendo las mejoras que corresponda.	Dpto. Proyectos
15	Especificaciones Técnicas e Interfaz	II / IE	Externo	Documentos que definen los lineamientos de la ingeniería de detalle que serán los pilares de la ingeniería de obra	Cliente
16	Memorias de Cálculo y/o Técnicas	II / IE	Externo	Documento que tiene los procedimientos descritos de forma detallada de cómo se realizaron los cálculos de las ingenierías que intervienen en el desarrollo de un proyecto	Cliente
17	Planos de diseño	II / IE	Externo	Documentos gráficos y escritos necesarios para la construcción del proyecto	Cliente
18	Lista de equipos	II / IE	Externo	Documento que enlista los equipos usados en el proyecto	Cliente
19	Hojas de Datos de Equipos	II / IE	Externo	Documento que resume las características técnicas de los equipos enlistados	Cliente
20	Certificados Técnicos.	II / IE	Externo	Documento que muestra las certificaciones y normas que cumple un equipo	Cliente

21	Informe de Novedades de Etapa de detalle	II / IE	Interno	Documento realizado por el equipo encargado de la fiscalización donde somete la ingeniería de detalle a una cuidadosa revisión, detectando las observaciones que merezca y proponiendo las mejoras que corresponda.	Dpto. Proyectos
22	Documento de Trazabilidad	II / IE	Interno	Documento se realiza el seguimiento de las observaciones realizadas en el informe de novedades, hasta su resolución	Dpto. Proyectos
23	Acta de reunión	II	Interno	Documento donde se relata los compromisos que adquieren cada una de las partes del proyecto luego de una mesa de trabajo	Dpto. Proyectos
24	Informe final de etapa de detalle	II / IE	Interno	Documento realizado por el equipo encargado de la fiscalización de la etapa de detalle donde da por finalizada esta etapa habiendo cumplido con las exigencias del proyecto y así empezar la eta de construcción	Dpto. Proyectos
25	Software de Ofimática	SW	Interno	Software para elaboración de documentos	Empresa
26	Software para visualización de planos	SW	Interno	Software para visualización de planos	Empresa
27	Almacenamiento en la Nube	SW	Interno	Espacio para almacenamiento de la información en la nube	Empresa

28	Equipo Tecnológico	HW	Interno	Equipos necesarios para realizar la fiscalización	Empresa
29	Personal del Dpto. Proyectos	PER	Interno	Personal que realiza fiscalización	Dpto. Proyectos
30	Personal del Dpto. Comercial	PER	Interno	Personal que realiza la gestión comercial de los proyectos	Dpto. Comercial
31	Correo Electrónico	SW	Interno	Software para intercambio de mensajes y documentos electrónicos	Empresa
32	Oficina	S	Interno	Instalaciones de la empresa	Empresa
33	Equipos Celulares	Hardware	Interno	Equipos de comunicación	Empresa
34	Transporte	Otros	Interno	Vehículos para transporte del personal	Empresa
35	Equipos de Protección Personal	Otros	Interno	Equipos de protección en campo del personal	Empresa
36	Software de simulación de Ingeniería	SW	Interno	Software para simulación de la ingeniería propuesta en el proyecto	Empresa

Fuente: Los Autores

3.3 EVALUACIÓN DE IMPACTO DE LOS ACTIVOS DE INFORMACIÓN.

Para realizar la evaluación de impacto de los activos de información, se utiliza los criterios establecidos de la Tabla 1, los propietarios de los activos deberán calificar los atributos de la información en una escala de 1 a 3, siendo 3 es el más alto impacto y 1 el nivel de impacto más bajo.

Para evaluar el criterio Confidencialidad se debe tener en consideración el nivel de confidencialidad que tiene la información de cada activo, considerando lo siguiente:

Tabla 6 Nivel de Confidencialidad

NIVEL	EQUIVALENCIA CUANTITATIVA	DESCRIPCIÓN
ALTO	3	Solo personal autorizado.
MEDIO	2	Dentro de la organización.
BAJO	1	Público

Fuente: Los Autores

Para evaluar el criterio Integridad se debe tener en consideración el nivel de integridad que tiene la información de cada activo, considerando lo siguiente:

Tabla 7 Nivel de Integridad

NIVEL	EQUIVALENCIA CUANTITATIVA	DESCRIPCIÓN
ALTO	3	Afectación total si existe daño.
MEDIO	2	Afectación parcial si existe daño.
BAJO	1	Sin afectación si existe daño.

Fuente: Los Autores

Para evaluar el criterio Disponibilidad se debe tener en consideración el nivel de disponibilidad que tiene la información de cada activo, considerando lo siguiente:

Tabla 8 Nivel de Disponibilidad

NIVEL	EQUIVALENCIA CUANTITATIVA	DESCRIPCIÓN

ALTO	3	Afectación total si no está accesible.
MEDIO	2	Afectación parcial si no está accesible.
BAJO	1	No afecta si no está accesible.

Fuente: Los Autores

Las calificaciones se promedian y se obtiene una calificación única para cada activo, luego se seleccionan solo los activos que promedien 3 (alto), es decir se considerarán a estos como activos críticos dentro del proceso evaluado, si estos activos fueran afectados negativamente, habría paralización o afectación en el flujo del proceso.

A continuación, se muestra la calificación realizada sobre el Inventario de Activos:

Tabla 9 Calificación de Activos

No.	Nombre del Activo	Tipo de Activo	Tipo	C	I	D	Impacto Cuantitativo	Impacto Cualitativo
1	Orden de Trabajo	IE	Interno	2	3	1	2	Medio
2	Bitácora de Trabajos	IE	Interno	3	3	3	3	Alto
3	Términos de Referencia	II / IE	Externo	1	3	2	2	Medio
4	Contrato de Obra	II	Externo	3	3	2	3	Alto
5	Memoria Técnica Preliminar	II	Externo	2	3	2	2	Medio
6	Especificaciones Funcionales	II	Externo	2	3	2	2	Medio
7	Planos de ubicación	II	Externo	2	3	2	2	Medio

8	Presupuesto referencial	II	Externo	3	3	2	3	Alto
9	Aval de recursos	IE	Interno	1	2	1	1	Bajo
10	Solicitud de asignación de recursos	IE	Interno	1	2	1	1	Bajo
11	Proceso de Adquisición de Recursos	P	Interno	2	2	1	2	Medio
12	Acta de Recepción	II	Interno	2	2	2	2	Medio
13	Acta de Inicio de fiscalización	II	Interno	3	2	2	2	Medio
14	Informe Preliminar del proyecto	II / IE	Interno	3	2	2	2	Medio
15	Especificaciones Técnicas e Interfaz	II / IE	Externo	2	3	2	2	Medio
16	Memorias de Cálculo y/o Técnicas	II / IE	Externo	2	3	2	2	Medio
17	Planos de diseño	II / IE	Externo	3	3	2	3	Alto
18	Lista de equipos	II / IE	Externo	2	2	2	2	Medio
19	Hojas de Datos de Equipos	II / IE	Externo	2	2	1	2	Medio
20	Certificados Técnicos.	II / IE	Externo	1	3	1	2	Medio
21	Informe de Novedades de Etapa de detalle	II / IE	Interno	3	3	2	3	Alto
22	Documento de Trazabilidad	II / IE	Interno	3	3	2	3	Alto
23	Acta de reunión	II	Interno	3	3	2	3	Alto
24	Informe final de etapa de detalle	II / IE	Interno	3	3	2	3	Alto
25	Software de Ofimática	SW	Interno	1	1	3	2	Medio

26	Software para visualización de planos	SW	Interno	1	2	3	2	Medio
27	Almacenamiento en la Nube	SW	Interno	3	3	3	3	Alto
28	Equipo Tecnológico	HW	Interno	2	2	3	2	Medio
29	Personal del Dpto. Proyectos	PER	Interno	1	1	3	2	Medio
30	Personal del Dpto. Comercial	PER	Interno	1	1	2	1	Bajo
31	Correo Electrónico	SW	Interno	3	3	3	3	Alto
32	Oficina	S	Interno	1	1	3	2	Medio
33	Equipos Celulares	Hardware	Interno	3	2	3	3	Alto
34	Transporte	Otros	Interno	1	1	3	2	Medio
35	Equipos de Protección Personal	Otros	Interno	1	1	2	1	Bajo
36	Software de simulación de Ingeniería	SW	Interno	3	2	3	3	Alto

Fuente: Los Autores

Al finalizar la evaluación, se extrae el Inventario de Activos Críticos, con los activos que hayan obtenido en promedio 3 (Alto):

Tabla 10 Inventario de Activos Críticos

No.	Nombre del Activo	Tipo de Activo	Tipo	C	I	D	Impacto Cuantitativo	Impacto Cualitativo
1	Bitácora de Trabajos	IE	Interno	3	3	3	3	Alto
2	Contrato de Obra	II	Externo	3	3	2	3	Alto
3	Presupuesto referencial	II	Externo	3	3	2	3	Alto

4	Planos de diseño	II / IE	Externo	3	3	2	3	Alto
5	Informe de Novedades de Etapa de detalle	II / IE	Interno	3	3	2	3	Alto
6	Documento de Trazabilidad	II / IE	Interno	3	3	2	3	Alto
7	Acta de reunión	II	Interno	3	3	2	3	Alto
8	Informe final de etapa de detalle	II / IE	Interno	3	3	2	3	Alto
9	Almacenamiento en la Nube	SW	Interno	3	3	3	3	Alto
10	Correo Electrónico	SW	Interno	3	3	3	3	Alto
11	Equipos Celulares	HW	Interno	3	2	3	3	Alto
12	Software de simulación de Ingeniería	SW	Interno	3	2	3	3	Alto

Fuente: Los Autores

3.4 INCIDENTES DE SEGURIDAD DETECTADOS.

Al obtener el Inventario de Activos Críticos, se pueden obtener las amenazas y vulnerabilidades de cada activo.

Una amenaza, es todo aquello que pueda explotar o evidenciar una vulnerabilidad con probabilidad de causar potencialmente incidentes sobre uno o más activos y comprometer a la organización. Las amenazas deben ser levantadas e identificadas por los propietarios de los activos considerando incidentes anteriores, así como también el Anexo C “Ejemplos de Amenazas Comunes” de la norma ISO/IEC 27005 [9]. Durante la identificación de amenazas se pueden usar métodos como: entrevistas, visitas, listas de verificación.

Ya que, al momento de la elaboración de este trabajo de investigación, no se han reportado o evidenciado en un registro formal las incidencias de seguridad, se adaptarán los ejemplos de las amenazas comunes según el Anexo C de la norma ISO/IEC 27005, una amenaza puede ser deliberada, natural, accidental o ambiental; las amenazas pueden afectar a cada activo de manera diferente.

A continuación, se detalla un listado que debe ser adaptado según el inventario de activos críticos presentes en el proceso analizado.

- Amenazas de origen físico:
    - Incendio.
    - Desastre (origen humano).
    - Desastre (origen natural).
    - Problemas eléctricos.
    - Mal funcionamiento de equipos.
    - Problemas ambientales (humedad, temperatura, polvo, ventilación).
    - Paralizaciones (Huelgas).

- Amenazas de origen criminal:
    - Robo.
    - Acceso físico no autorizado.
    - Vandalismo.
    - Espionaje corporativo.
    - Malversación.

    - Falsificación de registros.
    - Fraude.
    - Fuga de información.

- Amenazas de origen de Hardware:
    - Errores de mantenimiento.
    - Infección de virus a través de unidades extraíbles.
    - Pérdida de equipos.
    - Pérdida de datos por errores de hardware.

- Amenazas de origen de Software:
    - Código malicioso.
    - Interrupción de procesos de negocio.
    - Errores de software.
    - Información confidencial comprometida.
    - Software fraudulento.

- Amenazas de origen de Usuario:
    - Destrucción de registros.
    - Uso indebido de los sistemas de información.
    - Ingeniería social.
    - Cambio involuntario de datos.
    - Cambios no autorizados de registros.
    - Uso no autorizado de software.

    - Error de usuario.
    - Instalación no autorizada de software.

- Amenazas de origen político:
    - Incumplimiento de relaciones contractuales.
    - Incumplimiento de normas y reglas.
    - Errores de definición de roles de usuarios.

- Amenazas de origen de red:
    - Falla de los enlaces de comunicación.
    - Acceso a la red por personal no autorizado.
    - Red inalámbrica expuesta.
    - Daño causado por terceros.
    - Accesos no autorizados a los sistemas de información.

CAPÍTULO 4

DESARROLLO DEL ANÁLISIS DE RIESGOS

4.1 DETERMINACIÓN DE LAS AMENAZAS Y VULNERABILIDADES DEL PROCESO.

Como se lo ha mencionado, las amenazas son aquellos elementos que pueden causar daño sobre la información de un activo, estas pueden ser encontradas a partir de una vulnerabilidad presente. Una vulnerabilidad se refiere a las debilidades en un activo o en su entorno. Así, el riesgo es la probabilidad de que una amenaza explote una vulnerabilidad y genere impacto sobre un activo.

Para la identificación de las amenazas y vulnerabilidades del proceso evaluado, se debe tener en consideración aspectos internos y externos:

- La realidad organizacional.
- El ambiente regulatorio.
- Personal humano.
- Instalaciones físicas.
- Configuración de los sistemas de información, incluidos los operacionales y de aplicación.
- La tecnología en uso.

Se considera la siguiente Matriz de Amenazas y Vulnerabilidades de los activos críticos identificados del proceso evaluado, en esta matriz constan las vulnerabilidades que puedan ser explotadas por amenazas existentes, además se ha identificado en qué criterio de la información tendrá impacto la materialización de la amenaza.

Tabla 11 Matriz de Amenazas y Vulnerabilidades

No	Nombre del Activo	Tipo de Activo	Origen de Amenaza	Amenazas	Vulnerabilidades	C	I	D
1	Bitácora de Trabajos	IE	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
1	Bitácora de Trabajos	IE	Criminal	Falsificación de registros	Ausencia de control de cambios en el documento	X	X	
1	Bitácora de Trabajos	IE	Criminal	Fuga de información	Almacenamiento sin protección	X		
1	Bitácora de Trabajos	IE	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
1	Bitácora de Trabajos	IE	SW	Código malicioso	Inexistencia de software de seguridad	X	X	X
1	Bitácora de Trabajos	IE	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	

1	Bitácora de Trabajos	IE	Usuario	Destrucción de registros.	Uso incorrecto del aplicativo	X	X	X
1	Bitácora de Trabajos	IE	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
1	Bitácora de Trabajos	IE	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
1	Bitácora de Trabajos	IE	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
1	Bitácora de Trabajos	IE	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X		
1	Bitácora de Trabajos	IE	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X		
1	Bitácora de Trabajos	IE	Red	Daño causado por terceros.	Transmisión no cifrada de datos	X	X	X
2	Contrato de Obra	II	Físico	Incendio	Ubicación en un área susceptible			X
2	Contrato de Obra	II	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
2	Contrato de Obra	II	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
2	Contrato de Obra	II	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
2	Contrato de Obra	II	Criminal	Robo	Falta de protección física de la organización	X		X
2	Contrato de Obra	II	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
2	Contrato de Obra	II	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
2	Contrato de Obra	II	Criminal	Fuga de información	Almacenamiento sin protección	X		
2	Contrato de Obra	II	Usuario	Destrucción de registros.	Manipulación inadecuada del documento	X	X	
2	Contrato de Obra	II	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
2	Contrato de Obra	II	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
2	Contrato de Obra	II	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X

2	Contrato de Obra	II	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X		
3	Presupuesto referencial	II	Físico	Incendio	Ubicación en un área susceptible			X
3	Presupuesto referencial	II	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
3	Presupuesto referencial	II	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
3	Presupuesto referencial	II	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
3	Presupuesto referencial	II	Criminal	Robo	Falta de protección física de la organización	X		X
3	Presupuesto referencial	II	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
3	Presupuesto referencial	II	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
3	Presupuesto referencial	II	Criminal	Fuga de información	Almacenamiento sin protección	X		
3	Presupuesto referencial	II	Usuario	Destrucción de registros.	Manipulación inadecuada del documento	X	X	
3	Presupuesto referencial	II	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
3	Presupuesto referencial	II	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
3	Presupuesto referencial	II	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X
3	Presupuesto referencial	II	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X		
4	Planos de diseño	II / IE	Físico	Incendio	Ubicación en un área susceptible			X
4	Planos de diseño	II / IE	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
4	Planos de diseño	II / IE	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
4	Planos de diseño	II / IE	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
4	Planos de diseño	II / IE	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		

4	Planos de diseño	II / IE	Criminal	Falsificación de registros	Ausencia de control de cambios en el documento	X	X	
4	Planos de diseño	II / IE	Criminal	Fuga de información	Almacenamiento sin protección	X		
4	Planos de diseño	II / IE	Criminal	Robo	Falta de protección física de la organización			X
4	Planos de diseño	II / IE	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
4	Planos de diseño	II / IE	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
4	Planos de diseño	II / IE	SW	Código malicioso	Protección desactualizada contra códigos maliciosos.	X	X	X
4	Planos de diseño	II / IE	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	
4	Planos de diseño	II / IE	SW	Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		X	
4	Planos de diseño	II / IE	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
4	Planos de diseño	II / IE	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
4	Planos de diseño	II / IE	Usuario	Destrucción de registros.	Manipulación inadecuada del documento		X	X
4	Planos de diseño	II / IE	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
4	Planos de diseño	II / IE	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X	X	
4	Planos de diseño	II / IE	Red	Daño causado por terceros.	Contraseñas accesibles a personas no autorizadas.	X	X	X
4	Planos de diseño	II / IE	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X
4	Planos de diseño	II / IE	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
4	Planos de diseño	II / IE	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X	X	
5	Informe de Novedades de Etapa de detalle	II / IE	Físico	Incendio	Ubicación en un área susceptible			X

5	Informe de Novedades de Etapa de detalle	II / IE	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
5	Informe de Novedades de Etapa de detalle	II / IE	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
5	Informe de Novedades de Etapa de detalle	II / IE	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
5	Informe de Novedades de Etapa de detalle	II / IE	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
5	Informe de Novedades de Etapa de detalle	II / IE	Criminal	Falsificación de registros	Ausencia de control de cambios en el documento	X	X	
5	Informe de Novedades de Etapa de detalle	II / IE	Criminal	Fuga de información	Almacenamiento sin protección	X		
5	Informe de Novedades de Etapa de detalle	II / IE	Criminal	Robo	Falta de protección física de la organización			X
5	Informe de Novedades de Etapa de detalle	II / IE	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
5	Informe de Novedades de Etapa de detalle	II / IE	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
5	Informe de Novedades de Etapa de detalle	II / IE	SW	Código malicioso	Inexistencia de software de seguridad.	X	X	X
5	Informe de Novedades de Etapa de detalle	II / IE	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	
5	Informe de Novedades de Etapa de detalle	II / IE	SW	Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		X	
5	Informe de Novedades de Etapa de detalle	II / IE	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
5	Informe de Novedades de Etapa de detalle	II / IE	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
5	Informe de Novedades de Etapa de detalle	II / IE	Usuario	Destrucción de registros.	Manipulación inadecuada del documento		X	X
5	Informe de Novedades de Etapa de detalle	II / IE	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		

5	Informe de Novedades de Etapa de detalle	II / IE	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X	X	
5	Informe de Novedades de Etapa de detalle	II / IE	Red	Daño causado por terceros.	Transmisión no cifrada de datos	X	X	X
5	Informe de Novedades de Etapa de detalle	II / IE	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X
5	Informe de Novedades de Etapa de detalle	II / IE	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
5	Informe de Novedades de Etapa de detalle	II / IE	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X	X	
6	Documento de Trazabilidad	II / IE	Físico	Incendio	Ubicación en un área susceptible			X
6	Documento de Trazabilidad	II / IE	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
6	Documento de Trazabilidad	II / IE	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
6	Documento de Trazabilidad	II / IE	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
6	Documento de Trazabilidad	II / IE	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
6	Documento de Trazabilidad	II / IE	Criminal	Falsificación de registros	Ausencia de control de cambios en el documento	X	X	
6	Documento de Trazabilidad	II / IE	Criminal	Fuga de información	Almacenamiento sin protección	X		
6	Documento de Trazabilidad	II / IE	Criminal	Robo	Falta de protección física de la organización			X
6	Documento de Trazabilidad	II / IE	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
6	Documento de Trazabilidad	II / IE	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
6	Documento de Trazabilidad	II / IE	SW	Código malicioso	Falta de antivirus con licencia.	X	X	X
6	Documento de Trazabilidad	II / IE	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	
6	Documento de Trazabilidad	II / IE	SW	Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		X	

6	Documento de Trazabilidad	II / IE	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
6	Documento de Trazabilidad	II / IE	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
6	Documento de Trazabilidad	II / IE	Usuario	Destrucción de registros.	Manipulación inadecuada del documento		X	X
6	Documento de Trazabilidad	II / IE	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
6	Documento de Trazabilidad	II / IE	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X	X	
6	Documento de Trazabilidad	II / IE	Red	Daño causado por terceros.	Contraseñas inseguras.	X	X	X
6	Documento de Trazabilidad	II / IE	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X
6	Documento de Trazabilidad	II / IE	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
6	Documento de Trazabilidad	II / IE	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X	X	
7	Acta de reunión	II	Físico	Incendio	Ubicación en un área susceptible			X
7	Acta de reunión	II	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
7	Acta de reunión	II	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
7	Acta de reunión	II	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
7	Acta de reunión	II	Criminal	Robo	Falta de protección física de la organización	X		X
7	Acta de reunión	II	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
7	Acta de reunión	II	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
7	Acta de reunión	II	Criminal	Fuga de información	Almacenamiento sin protección	X		
7	Acta de reunión	II	Usuario	Destrucción de registros.	Manipulación inadecuada del documento	X	X	

7	Acta de reunión	II	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
7	Acta de reunión	II	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
7	Acta de reunión	II	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X
7	Acta de reunión	II	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X		
8	Informe final de etapa de detalle	II / IE	Físico	Incendio	Ubicación en un área susceptible			X
8	Informe final de etapa de detalle	II / IE	Físico	Desastre de origen humano	Manipulación inadecuada del documento			X
8	Informe final de etapa de detalle	II / IE	Físico	Desastre de origen natural	Ubicación en un área susceptible			X
8	Informe final de etapa de detalle	II / IE	Físico	Problemas ambientales	Ambiente susceptible a la humedad			X
8	Informe final de etapa de detalle	II / IE	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	X		
8	Informe final de etapa de detalle	II / IE	Criminal	Falsificación de registros	Ausencia de control de cambios en el documento	X	X	
8	Informe final de etapa de detalle	II / IE	Criminal	Fuga de información	Almacenamiento sin protección	X		
8	Informe final de etapa de detalle	II / IE	Criminal	Robo	Falta de protección física de la organización			X
8	Informe final de etapa de detalle	II / IE	Criminal	Acceso físico no autorizado	Copias del documento sin control	X		
8	Informe final de etapa de detalle	II / IE	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
8	Informe final de etapa de detalle	II / IE	SW	Código malicioso	Inexistencia de software de seguridad	X	X	X
8	Informe final de etapa de detalle	II / IE	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	
8	Informe final de etapa de detalle	II / IE	SW	Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		X	
8	Informe final de etapa de detalle	II / IE	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X

8	Informe final de etapa de detalle	II / IE	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
8	Informe final de etapa de detalle	II / IE	Usuario	Destrucción de registros.	Manipulación inadecuada del documento		X	X
8	Informe final de etapa de detalle	II / IE	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
8	Informe final de etapa de detalle	II / IE	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X	X	
8	Informe final de etapa de detalle	II / IE	Red	Daño causado por terceros.	Transmisión no cifrada de datos	X	X	X
8	Informe final de etapa de detalle	II / IE	Político	Incumplimiento de normas y reglas	Ausencia de documentación			X
8	Informe final de etapa de detalle	II / IE	Político	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	X		
8	Informe final de etapa de detalle	II / IE	Político	Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	X	X	
9	Almacenamiento en la Nube	SW	SW	Errores de Software	Sincronización inadecuada de los archivos	X	X	X
9	Almacenamiento en la Nube	SW	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	
9	Almacenamiento en la Nube	SW	Usuario	Destrucción de registros.	Manipulación inadecuada del documento		X	X
9	Almacenamiento en la Nube	SW	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
9	Almacenamiento en la Nube	SW	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
9	Almacenamiento en la Nube	SW	Usuario	Error de usuario	Manejo inadecuado de contraseñas	X	X	
9	Almacenamiento en la Nube	SW	Red	Falla de los enlaces de comunicación.	Inadecuada administración de la red			X
9	Almacenamiento en la Nube	SW	Red	Acceso a la red por personal no autorizado.	Falta de desactivación de cuentas de usuario cuando finaliza un contrato.	X	X	
9	Almacenamiento en la Nube	SW	Red	Daño causado por terceros.	Almacenamiento sin protección.	X	X	X
9	Almacenamiento en la Nube	SW	Red	Red inalámbrica expuesta	Red sin protección.	X	X	

10	Correo Electrónico	SW	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
10	Correo Electrónico	SW	SW	Errores de Software	Configuración incorrecta de parámetros		X	X
10	Correo Electrónico	SW	SW	Información confidencial comprometida	Información disponible a personas no autorizadas	X	X	X
10	Correo Electrónico	SW	SW	Código malicioso	Inexistencia de software de seguridad	X	X	X
10	Correo Electrónico	SW	Usuario	Destrucción de registros.	Manipulación inadecuada del servicio		X	X
10	Correo Electrónico	SW	Usuario	Error de usuario	Manejo inadecuado de contraseñas	X	X	
10	Correo Electrónico	SW	Usuario	Ingeniería social	Inadecuado nivel de concienciación de los empleados	X		
10	Correo Electrónico	SW	Político	Incumplimiento de normas y reglas	Inadecuado nivel de concienciación de los empleados	X		
10	Correo Electrónico	SW	Red	Falla de los enlaces de comunicación.	Inadecuada administración de la red			X
10	Correo Electrónico	SW	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X	X	
10	Correo Electrónico	SW	Red	Daño causado por terceros.	Transmisión no cifrada de datos	X	X	X
10	Correo Electrónico	SW	Red	Red inalámbrica expuesta	Red accesible a personas no autorizadas	X	X	
11	Equipos Celulares	HW	Físico	Desastre de origen humano	Manipulación inadecuada del dispositivo			X
11	Equipos Celulares	HW	Criminal	Robo	Falta de protección física de la organización			X
11	Equipos Celulares	HW	Criminal	Acceso físico no autorizado	Falta de control de accesibilidad al dispositivo	X	X	X
11	Equipos Celulares	HW	Criminal	Fuga de información	Falta de control del uso del dispositivo	X		
11	Equipos Celulares	HW	Criminal	Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados con el dispositivo	X		
11	Equipos Celulares	HW	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información del dispositivo		X	X
11	Equipos Celulares	HW	HW	Errores de mantenimiento	Mantenimiento insuficiente		X	X

11	Equipos Celulares	HW	HW	Pérdida de Equipos	Inadecuado nivel de concienciación de los empleados sobre el uso del dispositivo	X	X	X
11	Equipos Celulares	HW	SW	Código malicioso	Instalación de aplicaciones no autorizadas	X	X	X
11	Equipos Celulares	HW	SW	Errores de Software	Configuración incorrecta de parámetros		X	X
11	Equipos Celulares	HW	SW	Información confidencial comprometida	Uso de aplicaciones innecesarias.	X	X	X
11	Equipos Celulares	HW	Usuario	Destrucción de registros.	Manipulación inadecuada del dispositivo		X	X
11	Equipos Celulares	HW	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
11	Equipos Celulares	HW	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
11	Equipos Celulares	HW	Usuario	Uso no autorizado de software	Descarga y uso no controlado de software		X	
11	Equipos Celulares	HW	Político	Incumplimiento de normas y reglas	Inadecuado nivel de concienciación de los empleados	X		
11	Equipos Celulares	HW	Red	Acceso a la red por personal no autorizado.	Transmisión no cifrada de datos.	X	X	
11	Equipos Celulares	HW	Red	Daño causado por terceros.	Conexiones de red pública sin protección.	X	X	X
12	Software de simulación de Ingeniería	SW	HW	Pérdida de datos por errores de Hardware	No existen respaldos de la información		X	X
12	Software de simulación de Ingeniería	SW	HW	Infección de virus a través de unidades extraíbles	Falta de antivirus con licencia		X	X
12	Software de simulación de Ingeniería	SW	SW	Errores de Software	Configuración incorrecta de parámetros		X	X
12	Software de simulación de Ingeniería	SW	SW	Código malicioso	Inexistencia de software de seguridad	X	X	X
12	Software de simulación de Ingeniería	SW	SW	Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		X	

12	Software de simulación de Ingeniería	SW	Usuario	Destrucción de registros.	Manipulación inadecuada del software		X	X
12	Software de simulación de Ingeniería	SW	Usuario	Cambio involuntario de datos	Falta de manual de usuario		X	X
12	Software de simulación de Ingeniería	SW	Usuario	Cambios no autorizados de registros.	Falta de conocimiento del rol		X	X
12	Software de simulación de Ingeniería	SW	Usuario	Error de usuario	Falta de capacitación		X	X
12	Software de simulación de Ingeniería	SW	Red	Acceso a la red por personal no autorizado.	Redes sin acceso controlado	X	X	
12	Software de simulación de Ingeniería	SW	Red	Daño causado por terceros.	Transmisión no cifrada de datos	X	X	X

Fuente: Los Autores

4.2 ESTIMACION Y VALORACION DEL RIESGO.

Una vez que los riesgos han sido identificados, evaluaremos la probabilidad de ocurrencia de esos riesgos (amenaza + vulnerabilidad), a este paso se le denomina Valoración del riesgo y es el escalón preliminar para la identificación de los riesgos aceptables y el tratamiento que deben tener los riesgos inaceptables.

Se utilizan los valores de probabilidad e impacto de las Tablas 2 y 3 respectivamente, que fueron definidos con anterioridad. La evaluación de la probabilidad e impacto es subjetiva, podría asimismo ser producto del análisis de experiencia, históricos o lecciones aprendidas.

A continuación, se muestra la valoración de riesgos para cada uno de los activos críticos del proceso:

Nombre del Activo: Bitácora de Trabajo.

Tipo de Activo: Información Electrónica.

Tabla 12 Valoración de Riesgos - Bitácora de Trabajo.

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	MEDIO			MEDIO	SI	SI	SI
Falsificación de registros	Ausencia de control de cambios en el documento	MEDIO	ALTO		MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	MEDIO			ALTO	SI	SI	SI
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	ALTO	SI	NO	NO

Código malicioso	Inexistencia de software de seguridad	MEDIO	ALTO	MEDIO	MEDIO	SI	SI	SI
Información confidencial comprometida	Información disponible a personas no autorizadas	MEDIO	MEDIO		MEDIO	SI	SI	SI
Destrucción de registros.	Uso incorrecto del aplicativo	BAJO	ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		ALTO	ALTO	ALTO	SI	NO	NO
Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	ALTO	BAJO	SI	SI	SI

Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	MEDIO			MEDIO	SI	SI	SI
Daño causado por terceros.	Transmisión no cifrada de datos	ALTO	ALTO	ALTO	MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Contrato de Obra.

Tipo de Activo: Información Impresa.

Tabla 13 Valoración de Riesgos - Contrato de Obra

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible			ALTO	BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI

Robo	Falta de protección física de la organización	ALTO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	ALTO			MEDIO	SI	SI	SI
Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	MEDIO			MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			ALTO	NO	SI	SI
Destrucción de registros.	Manipulación inadecuada del documento	MEDIO	ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI

Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI
Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Presupuesto Referencial.

Tipo de Activo: Información Impresa.

Tabla 14 Valoración de Riesgos - Presupuesto Referencial

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible			ALTO	BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI

Robo	Falta de protección física de la organización	ALTO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	ALTO			MEDIO	SI	SI	SI
Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	MEDIO			MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			ALTO	NO	SI	SI
Destrucción de registros.	Manipulación inadecuada del documento	MEDIO	ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI

Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI
Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Planos de Diseño.

Tipo de Activo: Información Impresa e Información Electrónica.

Tabla 15 Valoración de Riesgos - Planos de Diseño

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible			ALTO	BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI

Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	ALTO			MEDIO	SI	SI	SI
Falsificación de registros	Ausencia de control de cambios en el documento	ALTO	ALTO		MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			MEDIO	SI	SI	SI
Robo	Falta de protección física de la organización	ALTO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	ALTO			MEDIO	SI	SI	SI
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	MEDIO	SI	SI	SI

Código malicioso	Protección desactualizada contra códigos maliciosos.	MEDIO	ALTO	MEDIO	MEDIO	SI	SI	SI
Información confidencial comprometida	Información disponible a personas no autorizadas	ALTO	MEDIO		ALTO	NO	SI	SI
Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		BAJO		MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		ALTO	BAJO	ALTO	SI	NO	SI
Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	BAJO	ALTO	SI	NO	SI

Destrucción de registros.	Manipulación inadecuada del documento		ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	ALTO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Contraseñas accesibles a personas no autorizadas.	ALTO	ALTO	MEDIO	ALTO	NO	NO	SI
Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI

Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Informe de Novedades de Etapa de Detalle.

Tipo de Activo: Información Impresa e Información Electrónica.

Tabla 16 Valoración de Riesgos - Informe de Novedades de Etapa de Detalle

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible				BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI
Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	ALTO			MEDIO	SI	SI	SI

Falsificación de registros	Ausencia de control de cambios en el documento	ALTO	ALTO		MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			MEDIO	SI	SI	SI
Robo	Falta de protección física de la organización	ALTO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	MEDIO			MEDIO	SI	SI	SI
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	MEDIO	SI	SI	SI
Código malicioso	Inexistencia de software de seguridad	MEDIO	ALTO	MEDIO	MEDIO	SI	SI	SI
Información confidencial comprometida	Información disponible a personas no autorizadas	ALTO	MEDIO		ALTO	NO	SI	SI

Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		BAJO		MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		ALTO	BAJO	ALTO	SI	NO	SI
Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	BAJO	ALTO	SI	NO	SI
Destrucción de registros.	Manipulación inadecuada del documento		ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	ALTO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Transmisión no cifrada de datos	ALTO	ALTO	MEDIO	ALTO	NO	NO	SI

Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI
Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Documento de Trazabilidad.

Tipo de Activo: Información Impresa e Información Electrónica.

Tabla 17 Valoración de Riesgos - Documento de Trazabilidad

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible			ALTO	BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI

Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	ALTO			MEDIO	SI	SI	SI
Falsificación de registros	Ausencia de control de cambios en el documento	ALTO	ALTO		MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			MEDIO	SI	SI	SI
Robo	Falta de protección física de la organización	ALTO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	MEDIO			MEDIO	SI	SI	SI
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	MEDIO	SI	SI	SI
Código malicioso	Falta de antivirus con licencia	MEDIO	ALTO	MEDIO	MEDIO	SI	SI	SI

Información confidencial comprometida	Información disponible a personas no autorizadas	ALTO	MEDIO		ALTO	NO	SI	SI
Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		BAJO		MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		ALTO	BAJO	ALTO	SI	NO	SI
Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	BAJO	ALTO	SI	NO	SI
Destrucción de registros.	Manipulación inadecuada del documento		ALTO	ALTO	ALTO	SI	NO	NO

Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	ALTO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Contraseñas inseguras.	ALTO	ALTO	MEDIO	ALTO	NO	NO	SI
Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI
Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Acta de Reunión.

Tipo de Activo: Información Impresa.

Tabla 18 Valoración de Riesgos - Acta de Reunión

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible			ALTO	BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI

Robo	Falta de protección física de la organización	MEDIO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	MEDIO			MEDIO	SI	SI	SI
Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	ALTO			MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			ALTO	NO	SI	SI
Destrucción de registros.	Manipulación inadecuada del documento		ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI

Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI
Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Informe Final de Etapa de Detalle.

Tipo de Activo: Información Impresa e Información Electrónica.

Tabla 19 Valoración de Riesgos - Informe Final de Etapa de Detalle

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Incendio	Ubicación en un área susceptible			ALTO	BAJO	SI	SI	SI
Desastre de origen humano	Manipulación inadecuada del documento			MEDIO	ALTO	SI	SI	SI
Desastre de origen natural	Ubicación en un área susceptible			MEDIO	MEDIO	SI	SI	SI
Problemas ambientales	Ambiente susceptible a la humedad			MEDIO	MEDIO	SI	SI	SI
Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados	ALTO			MEDIO	SI	SI	SI

Falsificación de registros	Ausencia de control de cambios en el documento	ALTO	ALTO		MEDIO	SI	SI	SI
Fuga de información	Almacenamiento sin protección	ALTO			MEDIO	SI	SI	SI
Robo	Falta de protección física de la organización	ALTO		ALTO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Copias del documento sin control	MEDIO			MEDIO	SI	SI	SI
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	MEDIO	SI	SI	SI
Código malicioso	Inexistencia de software de seguridad	MEDIO	ALTO	MEDIO	MEDIO	SI	SI	SI
Información confidencial comprometida	Información disponible a personas no autorizadas	ALTO	MEDIO		ALTO	NO	SI	SI

Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		BAJO		MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		ALTO	BAJO	ALTO	SI	NO	SI
Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	BAJO	ALTO	SI	NO	SI
Destrucción de registros.	Manipulación inadecuada del documento		ALTO	ALTO	ALTO	SI	NO	NO
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	ALTO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Transmisión no cifrada de datos	ALTO	ALTO	MEDIO	ALTO	NO	NO	SI

Incumplimiento de normas y reglas	Ausencia de documentación			ALTO	ALTO	SI	SI	NO
Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores	MEDIO			MEDIO	SI	SI	SI
Errores en la definición de roles de usuarios.	Reglas de acceso no definidas con claridad	MEDIO			MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Almacenamiento en la Nube.

Tipo de Activo: Software.

Tabla 20 Valoración de Riesgos - Almacenamiento en la Nube

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Errores de Software	Sincronización inadecuada de los archivos		ALTO	ALTO	ALTO	SI	NO	NO
Información confidencial comprometida	Información disponible a personas no autorizadas	ALTO	MEDIO		ALTO	NO	SI	SI
Destrucción de registros.	Manipulación inadecuada del documento		ALTO	ALTO	ALTO	SI	NO	NO
Cambio involuntario de datos	Falta de manual de usuario		ALTO	BAJO	ALTO	SI	NO	SI

Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	BAJO	MEDIO	SI	SI	SI
Error de usuario	Manejo inadecuado de contraseñas	ALTO	MEDIO		MEDIO	SI	SI	SI
Falla de los enlaces de comunicación .	Inadecuada administración de la red			ALTO	MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Falta de desactivación de cuentas de usuario cuando finaliza un contrato.	ALTO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Almacenamiento sin protección.	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI
Red inalámbrica expuesta	Red sin protección.	MEDIO	MEDIO		MEDIO	SI	SI	SI

Nombre del Activo: Correo Electrónico.

Tipo de Activo: Software.

Tabla 21 Valoración de Riesgos - Correo Electrónico

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	ALTO	SI	NO	NO
Errores de Software	Configuración incorrecta de parámetros		MEDIO	MEDIO	MEDIO	SI	SI	SI
Información confidencial comprometida	Información disponible a personas no autorizadas	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI
Código malicioso	Inexistencia de software de seguridad	ALTO	ALTO	BAJO	ALTO	NO	NO	SI

Destrucción de registros.	Manipulación inadecuada del servicio		ALTO	BAJO	MEDIO	SI	SI	SI
Error de usuario	Manejo inadecuado de contraseñas	ALTO	MEDIO		MEDIO	SI	SI	SI
Ingeniería social	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Incumplimiento de normas y reglas	Inadecuado nivel de concienciación de los empleados	ALTO			MEDIO	SI	SI	SI
Falla de los enlaces de comunicación.	Inadecuada administración de la red			MEDIO	MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	MEDIO	MEDIO		MEDIO	SI	SI	SI

Daño causado por terceros.	Transmisión no cifrada de datos	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI
Red inalámbrica expuesta	Red accesible a personas no autorizadas	ALTO	MEDIO		MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Equipos Celulares.

Tipo de Activo: Hardware.

Tabla 22 Valoración de Riesgos - Equipos Celulares

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Desastre de origen humano	Manipulación inadecuada del dispositivo			ALTO	ALTO	SI	SI	NO
Robo	Falta de protección física de la organización			MEDIO	MEDIO	SI	SI	SI
Acceso físico no autorizado	Falta de control de accesibilidad al dispositivo	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI
Fuga de información	Falta de control del uso del dispositivo	ALTO			ALTO	NO	SI	SI

Espionaje Corporativo	Inadecuada supervisión del trabajo de los empleados con el dispositivo	MEDIO			MEDIO	SI	SI	SI
Pérdida de datos por errores de Hardware	No existen respaldos de la información del dispositivo		MEDIO	MEDIO	MEDIO	SI	SI	SI
Errores de mantenimiento	Mantenimiento insuficiente		ALTO	ALTO	ALTO	SI	NO	NO
Pérdida de Equipos	Inadecuado nivel de concienciación de los empleados sobre el uso del dispositivo	MEDIO	ALTO	ALTO	ALTO	SI	NO	NO
Código malicioso	Instalación de aplicaciones no autorizadas	MEDIO	MEDIO	MEDIO	MEDIO	SI	SI	SI

Errores de Software	Configuración incorrecta de parámetros		MEDIO	MEDIO	MEDIO	SI	SI	SI
Información confidencial comprometida	Uso de aplicaciones innecesarias.	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI
Destrucción de registros.	Manipulación inadecuada del dispositivo		MEDIO	ALTO	MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		MEDIO	ALTO	MEDIO	SI	SI	SI
Cambios no autorizados de registros.	Falta de conocimiento del rol		MEDIO	ALTO	MEDIO	SI	SI	SI
Uso no autorizado de software	Descarga y uso no controlado de software		MEDIO		ALTO	SI	SI	SI

Incumplimiento de normas y reglas	Inadecuado nivel de concienciación de los empleados	MEDIO			MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Transmisión no cifrada de datos	MEDIO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Conexiones de red pública sin protección.	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI

Fuente: Los Autores

Nombre del Activo: Software de Simulación de Ingeniería.

Tipo de Activo: Software.

Tabla 23 Valoración de Riesgos - Software de Simulación de Ingeniería

Amenaza	Vulnerabilidad	IMPACTO			Probabilidad	RIESGO ACEPTABLE		
		C	I	D		R - C	R - I	R - D
Pérdida de datos por errores de Hardware	No existen respaldos de la información		ALTO	ALTO	ALTO	SI	NO	NO
Infección de virus a través de unidades extraíbles	Falta de antivirus con licencia		MEDIO	MEDIO	MEDIO	SI	SI	SI
Errores de Software	Configuración incorrecta de parámetros		ALTO	MEDIO	MEDIO	SI	SI	SI
Código malicioso	Inexistencia de software de seguridad	ALTO	ALTO	BAJO	ALTO	NO	NO	SI

Software fraudulento	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales		ALTO		MEDIO	SI	SI	SI
Destrucción de registros.	Manipulación inadecuada del software		MEDIO	ALTO	MEDIO	SI	SI	SI
Cambio involuntario de datos	Falta de manual de usuario		ALTO	MEDIO	ALTO	SI	NO	SI
Cambios no autorizados de registros.	Falta de conocimiento del rol		ALTO	BAJO	ALTO	SI	NO	SI
Error de usuario	Falta de capacitación		MEDIO	MEDIO	MEDIO	SI	SI	SI
Acceso a la red por personal no autorizado.	Redes sin acceso controlado	MEDIO	MEDIO		MEDIO	SI	SI	SI
Daño causado por terceros.	Transmisión no cifrada de datos	ALTO	ALTO	MEDIO	MEDIO	SI	SI	SI

Fuente: Los Autores

4.3 IDENTIFICACIÓN DE RIESGOS CRÍTICOS.

Considerando los criterios de vulnerabilidad y probabilidad de ocurrencia, se identifican los riesgos críticos como aquellos cuyos niveles de impacto y probabilidad sea mayor a 2 (ALTO). Los riesgos con dicho valor se consideran como inaceptables y deben ser tratados en el siguiente capítulo.

En la siguiente tabla se resumen los riesgos críticos del proceso de Fiscalización de Proyectos de Ingeniería en la Etapa de Detalle.

Tabla 24 Riesgos Críticos del Proceso de Fiscalización de Proyectos de Ingeniería en la Etapa de Detalle

Nombre del Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo Inaceptable en C, I o D
Bitácora de Trabajos / Correo Electrónico / Software de Simulación de Ingeniería	Pérdida de datos por errores de Hardware	No existen respaldos de la información	I, D
Bitácora de Trabajos	Destrucción de registros.	Uso incorrecto del aplicativo	I, D
Contrato de Obra / Presupuesto Referencial / Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Acta de Reunión / Informe Final de Etapa de Detalle / Almacenamiento en la Nube	Destrucción de registros.	Manipulación inadecuada del documento	I, D
Bitácora de Trabajos	Cambio involuntario de datos	Falta de manual de usuario	I, D

Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Almacenamiento en la Nube / Software de Simulación de Ingeniería	Cambio involuntario de datos	Falta de manual de usuario	I
Contrato de Obra / Presupuesto Referencial / Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Acta de Reunión / Informe Final de Etapa de Detalle	Incumplimiento de normas y reglas	Ausencia de documentación	D
Presupuesto Referencial / Acta de Reunión	Fuga de información	Almacenamiento sin protección	C
Equipos Celulares	Fuga de información	Falta de control del uso del dispositivo	C
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Almacenamiento en la Nube	Información confidencial comprometida	Información disponible a personas no autorizadas	C
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Software de Simulación de Ingeniería	Cambios no autorizados de registros.	Falta de conocimiento del rol	I
Planos de Diseño	Daño causado por terceros.	Contraseñas accesibles a personas no autorizadas.	C, I
Informe de Novedades de Etapa de Detalle / Informe Final de Etapa de Detalle	Daño causado por terceros.	Transmisión no cifrada de datos	C, I
Documento de Trazabilidad	Daño causado por terceros.	Contraseñas inseguras.	C, I

Almacenamiento en la Nube	Errores de Software	Sincronización inadecuada de los archivos	I, D
Correo Electrónico / Software de Simulación de Ingeniería	Código malicioso	Inexistencia de software de seguridad	C, I
Equipos Celulares	Desastre de origen humano	Manipulación inadecuada del dispositivo	D
Equipos Celulares	Errores de mantenimiento	Mantenimiento insuficiente	I, D
Equipos Celulares	Pérdida de Equipos	Inadecuado nivel de concienciación de los empleados sobre el uso del dispositivo	I, D

Fuente: Los Autores

CAPÍTULO 5

TRATAMIENTO DEL RIESGO

5.1 DETERMINAR LAS ESTRATEGIAS DE RESPUESTAS A LOS RIESGOS.

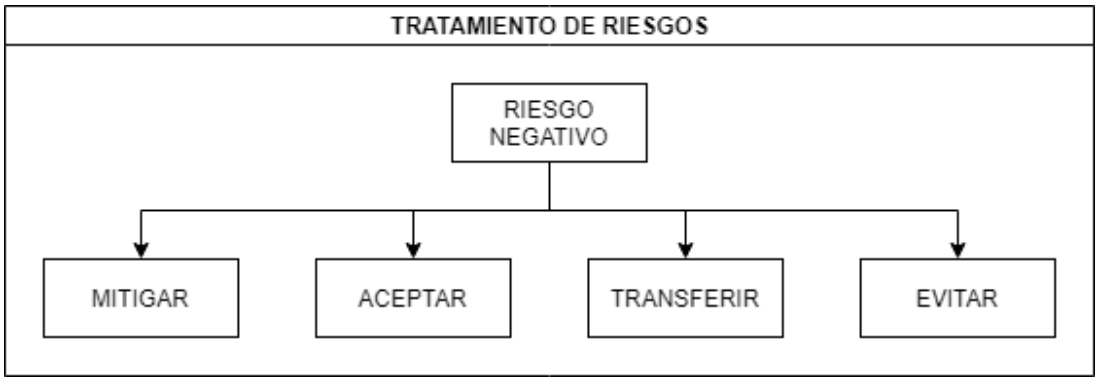
El tratamiento del riesgo implica el enfoque en la toma de decisiones sobre cómo se abordan los riesgos encontrados en los activos críticos.

Si estos riesgos representan pérdida de valor sobre el activo, es decir que son riesgos negativos, se toma como referencia las siguientes opciones de respuestas las cuales pueden ocurrir simultáneamente:

- MITIGAR
- ACEPTAR

- TRANSFERIR
- EVITAR

Figura 5. 1 Tratamiento de Riesgos



Fuente: Los Autores

Si la decisión es **MITIGAR**, se implementan acciones que contrarresten la amenaza y resuelvan su origen; los riesgos que se mitigan suelen tener alto impacto en el proceso u organización. Mitigar el riesgo implica la elección de Controles de Seguridad de la Información.

Si la decisión es **ACEPTAR**, se está consciente de las consecuencias que pueda dejar la materialización de la amenaza o vulnerabilidad, para la aceptación del riesgo es importante contar con recursos en la organización ante la posible eventualidad y justificar la no utilización de controles para su tratamiento.

Si la decisión es **TRANSFERIR**, el riesgo es asignado a otra parte externa que pueda darle el tratamiento adecuado, sin embargo, esto puede modificar el riesgo ya existente. La transferencia se la puede hacer mediante subcontratación para que el riesgo sea monitoreado y se tomen acciones para

detener un evento antes de que se produzca daño en el proceso o en la organización.

Si la decisión es **EVITAR**, se eliminan o detienen por completo las actividades que originan el riesgo ya que se considera que el costo de tratarlo es mucho mayor al beneficio obtenido.

5.2 DETERMINAR LOS CONTROLES APLICABLES.

Para la identificación de controles, se seguirá la norma ISO/IEC 27002. El estándar ISO 27002 describe los controles de seguridad para dar a las organizaciones las mejores prácticas para un SGSI. El estándar 27002:2013 consiste de 3 capas ISO [18]:

- Capa I: 14 capítulos ISO - Dominios: Áreas funcionales de seguridad.
- Capa II: 35 subcapítulos ISO - Objetivos de control: Reflejan lo que se intenta conseguir.
- Capa III: 114 controles ISO - Conjunto de acciones, procedimientos, medidas técnicas o documentos que se deberán implementar para llegar a los objetivos.

Para la selección de controles se debe considerar aspectos como:

- El coste de implementación del control vs el coste de materialización de la amenaza/vulnerabilidad,
- Necesidad de disponibilidad del control,

- Controles existentes,
- Recursos económicos y humanos que implican la implementación del control.

Los controles serán aplicados para llevar al riesgo a un nivel aceptable o al mínimo posible. Los controles asociados, así como los que se escogieron para los activos con riesgo inaceptable, se los ha listado en el Informe de Tratamiento de Riesgos que se muestra a continuación:

Tabla 25 Informe de Tratamiento de Riesgos

Nombre del Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo Inaceptable en C, I o D	Alternativas de Tratamiento	Controles Asociados	Alternativa de Tratamiento Seleccionada
Bitácora de Trabajos / Correo Electrónico / Software de Simulación de Ingeniería	Perdida de datos por errores de Hardware	No existen respaldos de la información	I, D	MITIGAR	A.12.3.1	MITIGAR A.12.3.1
Bitácora de Trabajos	Destrucción de registros.	Uso incorrecto del aplicativo	I, D	MITIGAR	A.12.1.1 A.12.3.1 A.12.4.2	MITIGAR A.12.1.1
Contrato de Obra / Presupuesto Referencial / Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Acta de Reunión / Informe Final de Etapa de Detalle / Almacenamiento en la Nube	Destrucción de registros.	Manipulación inadecuada del documento	I, D	MITIGAR ACEPTAR	A.8.2.3 A.12.1.1 A.12.3.1 A.12.4.2	MITIGAR A.8.2.3
Bitácora de Trabajos	Cambio involuntario de datos	Falta de manual de usuario	I, D	MITIGAR	A.12.1.1 A.12.1.2 A.12.3.1	MITIGAR A.12.1.1

Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Almacenamiento en la Nube / Software de Simulación de Ingeniería	Cambio involuntario de datos	Falta de manual de usuario	I	MITIGAR	A.12.1.1 A.12.1.2 A.12.3.1	MITIGAR A.12.1.1
Contrato de Obra / Presupuesto Referencial / Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Acta de Reunión / Informe Final de Etapa de Detalle	Incumplimiento de normas y reglas	Ausencia de documentación	D	MITIGAR	A.7.1.2 A.7.2.2 A.7.2.3 A.8.1.3 A.9.1.1 A.12.1.1	MITIGAR A.12.1.1
Presupuesto Referencial / Acta de Reunión	Fuga de información	Almacenamiento sin protección	C	MITIGAR	A.7.1.2 A.7.2.2 A.7.2.3 A.9.1.1 A.9.2.3 A.9.4.1 A.13.2.4 A.18.1.3	MITIGAR A.9.4.1

Equipos Celulares	Fuga de información	Falta de control del uso del dispositivo	C	MITIGAR ACEPTAR	A.6.2.1 A.7.1.2 A.7.2.2 A.7.2.3 A.8.1.3 A.11.2.6 A.12.1.1 A.12.4.1 A.13.2.4 A.14.1.2	MITIGAR A.6.2.1
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Almacenamiento en la Nube	Información confidencial comprometida	Información disponible a personas no autorizadas	C	MITIGAR ACEPTAR	A.6.1.5 A.7.2.2 A.8.1.3 A.8.2.2 A.8.2.3 A.9.2.5 A.9.4.1 A.12.4.1 A.13.2.4	MITIGAR A.9.2.5
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Software de Simulación de Ingeniería	Cambios no autorizados de registros.	Falta de conocimiento del rol	I	MITIGAR	A.7.1.2 A.7.2.2 A.7.2.3 A.8.1.3 A.12.1.1 A.12.4.1 A.18.1.3	MITIGAR A.7.1.2

Planos de Diseño	Daño causado por terceros.	Contraseñas accesibles a personas no autorizadas.	C, I	MITIGAR	A.7.3.1 A.9.1.1 A.9.1.2 A.9.2.1 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6 A.9.3.1 A.9.4.1 A.9.4.3 A.11.2.8 A.12.4.1	MITIGAR A.11.2.8
Informe de Novedades de Etapa de Detalle / Informe Final de Etapa de Detalle	Daño causado por terceros.	Transmisión no cifrada de datos	C, I	MITIGAR	A.9.1.2 A.10.1.1 A.12.4.1 A.13.1.1 A.13.1.2	MITIGAR A.10.1.1
Documento de Trazabilidad	Daño causado por terceros.	Contraseñas inseguras.	C, I	MITIGAR	A.9.1.2 A.9.2.3 A.9.3.1 A.9.4.2 A.9.4.3	MITIGAR A.9.4.3

Almacenamiento en la Nube	Errores de Software	Sincronización inadecuada de los archivos	I, D	MITIGAR ACEPTAR	A.12.3.1 A.12.4.1 A.12.4.4	ACEPTAR Se acepta el riesgo ya que el Software para Almacenamiento en la Nube es responsabilidad del proveedor
Correo Electrónico / Software de Simulación de Ingeniería	Código malicioso	Inexistencia de software de seguridad	C, I	MITIGAR	A.12.2.1 A.12.6.2 A.13.2.3	MITIGAR A.12.2.1
Equipos Celulares	Desastre de origen humano	Manipulación inadecuada del dispositivo	D	MITIGAR ACEPTAR	A.6.2.1 A.7.2.2 A.8.1.3 A.11.2.6	MITIGAR A.6.2.1
Equipos Celulares	Errores de mantenimiento	Mantenimiento insuficiente	I, D	MITIGAR TRANSFERIR	A.6.2.1 A.11.2.4	TRANSFERIR A.11.2.4
Equipos Celulares	Perdida de Equipos	Inadecuado nivel de concienciación de los empleados sobre el uso del dispositivo	I, D	MITIGAR	A.6.2.1 A.7.1.2 A.7.2.2 A.8.1.3 A.11.2.6	MITIGAR A.6.2.1

Fuente: Los Autores

5.3 DETERMINAR LOS PROYECTOS PARA CERRAR LA BRECHA DE SEGURIDAD ENCONTRADA.

Luego de haber tomado la decisión sobre cómo tratar cada riesgo, se debe establecer el Plan de Tratamiento de Riesgos en donde se definen los responsables que implementarán los controles, así como también se calendariza la implementación de cada uno de estos en un Plan de Acción. El plan se ordenará en función al impacto que tendrán los controles sobre el proceso/organización.

Según el informe de tratamiento del riesgo, un mismo control puede ser implementado para varias amenazas/vulnerabilidades.

- **MITIGAR A.6.2.1**

Control: Política de Dispositivos Móviles.

Elaboración de Política interna para uso de dispositivos móviles, se deben definir los requerimientos y configuraciones de teléfonos inteligentes, tablets y computadores portátiles asignadas por la empresa y que intervienen en el proceso analizado. Las actividades realizadas en estos dispositivos móviles deben estar dentro del campo de acción asignado y por ningún motivo estos equipos deben ser usados para otros ámbitos que no sea el laboral, la data que se transmite a través de ellos debe realizarse solo sobre redes seguras y no haciendo uso de redes públicas.

Lo establecido en la Política debe ser socializado y posteriormente cumplido por todo el personal involucrado, es decir, todos quienes intervienen en el proceso.

- **MITIGAR A.7.12**

Control: Términos y Condiciones del Empleo.

Los contratos de los empleados deberán cubrir sus obligaciones y responsabilidades haciendo referencia a cada una de las cláusulas y políticas de restricción de la empresa.

- **MITIGAR A.8.2.3**

Control: Manipulado de la información.

Establecer el procedimiento de manipulación de información, en el que se defina cómo debe ser usada o manipulada la información categorizado como confidencial.

Se debe destacar que la información impresa también debe ser manipulada de forma segura, documentos con información sensible no deben mantenerse expuestos sobre escritorios o impresoras. La documentación que no necesita ser usada nuevamente o fue impresa por error, debe ser correctamente destruida.

- **MITIGAR A.9.2.5**

Control: Revisión de los derechos de acceso de usuario.

Establecer un procedimiento formal que ayude con la revisión de los derechos de usuario en intervalos regulares, en el que también se incluya la actualización del estado de los usuarios como cambios de departamento o vacaciones para las restricciones de accesos en documentos o aplicativos según corresponda.

- **MITIGAR A.9.4.1**

Control: Restricción del acceso a la información.

Establecer una Política de acceso y restricción a la información, en la que se incluyan los procedimientos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información de acuerdo a su clasificación, ya sea en forma impresa, digital, almacenada en la Nube o en dispositivos móviles.

Como parte de la Política, se requiere se implemente un Acuerdo de Confidencialidad para acordar entre las partes el buen uso de los activos, incluir sanciones en el caso del mal uso de la información/activo.

- **MITIGAR A.9.4.3**

Control: Sistema de Gestión de Contraseñas.

La asignación de contraseñas debe realizarse a través de un sistema de generación de contraseñas robustas, que permita llevar el control de contraseñas asignadas para que luego en un periodo no mayor a 3 meses, las contraseñas sean revocadas, obligando así al usuario a solicitar una nueva contraseña. Una vez asignada la contraseña de acceso a los diferentes servicios

(correo electrónico, almacenamiento en la Nube, equipos informáticos, software de simulación), el usuario es responsable del buen uso de la misma.

- **MITIGAR A.10.1.1**

Control: Política de uso de los controles criptográficos.

Establecer una Política de uso de controles criptográficos para el envío de información sensible usando algoritmos de cifrado. La contraseña para cifrado y descifrado debe ser manejada y almacenada de forma segura, accesible solo para quien sea permitido según se defina en la Política de acceso y restricción a la información.

- **TRANSFERIR A.11.2.4**

Control: Mantenimiento de los Equipos.

Este control se transfiere a un ente externo a la Empresa, sin embargo, se debe establecer un cronograma de mantenimiento periódico que permita llevar el control de forma interna. El riesgo aun transferido sigue siendo responsabilidad de la Empresa.

- **MITIGAR A.11.2.8**

Control: Equipo de usuario desatendido

Establecer el procedimiento de protección de equipos desatendidos, entre las medidas a implementar están:

- Bloqueo de pantalla manual cuando el usuario deje el puesto de trabajo de forma momentánea,

- Bloqueo de pantalla automático después de un periodo determinado de inactividad,
- Protectores de pantalla corporativos con contraseña,
- Cierre de sesión al finalizar jornada laboral.

- **MITIGAR A.12.1.1**

Control: Documentación de Procedimientos Operacionales.

Todos los procedimientos operacionales y políticas a establecer, deben estar correctamente documentados. Estos documentos además de ser socializados, deben permanecer almacenados en repositorios accesibles a los usuarios según los perfiles de acceso definidos en la Política de Acceso y Restricción a la Información y deben ser manipulados según el procedimiento correspondiente.

- **MITIGAR A.12.2.1**

Control: Controles contra el código malicioso.

Entre los controles a implementar se tienen:

- Uso de antivirus actualizado con licencias válidas.
- Restricción de navegación en sitios no seguros o con contenido malicioso.
- Contar con un procedimiento de respaldo de información.

- **MITIGAR A.12.3.1**

Control: Copias de Seguridad de la Información.

Definir los procedimientos para mantener respaldos de la información concerniente a los proyectos realizados de forma física y digital, según sean necesario se deberá guardar la copia de un número determinado de versiones de cada proyecto. El procedimiento debe incluir responsables de su custodia en el caso de los respaldos físicos y en el caso de los respaldos digitales el procedimiento debe indicar donde se almacenan y cómo se accede a la plataforma de almacenamiento.

- **CONTROL ADICIONAL A IMPLEMENTAR - A.7.2.2**

Control: Concienciación, educación y capacitación en seguridad de la información. (Oportunidad de Mejora)

Este control consiste en la socialización recurrente de las políticas, procedimientos y uso de las herramientas del proceso, el alcance de la capacitación depende del rol del empleado y sus responsabilidades asignadas. El control no abarca la creación de políticas ya que, para la socialización, estas ya deberían estar creadas.

La siguiente tabla denominada “Plan de Tratamiento 01” reúne los controles aplicables sobre los riesgos valorados, estos serán aplicados en el corto plazo en el periodo de tiempo propuesto de acuerdo a su impacto sobre los activos. Asimismo, se ha establecido los productos que tendrán cada uno de estos controles a aplicar.

Tabla 26 Plan de Tratamiento 01

Nombre del Activo	Amenaza	Vulnerabilidad	Alternativa de Tratamiento Seleccionada	Responsable de Actividad	Recursos	Presupuesto	Tiempo de Implementación	Plan de Acción	Evidencias Esperadas
Correo Electrónico / Software de Simulación de Ingeniería	Código malicioso	Inexistencia de software de seguridad	MITIGAR A.12.2.1	Dep. Tecnología	Personas. Tiempo. Dinero.	$500.00	1 semana	Adquisición de Software antivirus.	Licencias: Software Antivirus
Presupuesto Referencial / Acta de Reunión	Fuga de información	Almacenamiento sin protección	MITIGAR A.9.4.1	Jefes Técnicos	Personas. Tiempo.	$0.00	3 semanas	Elaboración de Política de acceso y restricción a la información.	Documentos: Política de Acceso y Restricción a la Información. Acuerdos de Confidencialidad.
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Almacenamiento en la Nube	Información confidencial comprometida	Información disponible a personas no autorizadas	MITIGAR A.9.2.5	Jefes Técnicos	Personas. Tiempo.	$0.00	8 días	Elaboración de procedimiento de revisión de derechos de usuario.	Documento: Procedimiento de Revisión de Derechos de Usuario.
Planos de Diseño	Daño causado por terceros.	Contraseñas accesibles a personas no autorizadas.	MITIGAR A.11.2.8	Dep. Tecnología	Personas. Tiempo.	$0.00	2 semanas	Elaboración de Procedimiento de protección de equipos desatendidos.	Documento: Procedimiento de Protección de Equipos Desatendidos.
Contrato de Obra / Presupuesto Referencial / Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Acta de Reunión / Informe Final de Etapa de Detalle / Almacenamiento en la Nube	Destrucción de registros.	Manipulación inadecuada del documento	MITIGAR A.8.2.3	Dep. Ingeniería	Personas. Tiempo.	$0.00	3 semanas	Elaboración de procedimiento de manipulación de información confidencial.	Documento: Procedimiento de Manipulación de Información Confidencial.

Bitácora de Trabajos / Correo Electrónico / Software de Simulación de Ingeniería	Perdida de datos por errores de Hardware	No existen respaldos de la información	MITIGAR A.12.3.1	Dep. Tecnología	Personas. Tiempo.	$0.00	3 semanas	Elaboración de procedimientos de copias de seguridad (Físico y digital)	Documentos: Procedimientos de respaldos de información.
Informe de Novedades de Etapa de Detalle / Informe Final de Etapa de Detalle	Daño causado por terceros.	Transmisión no cifrada de datos	MITIGAR A.10.1.1	Dep. Tecnología	Personas. Tiempo.	$0.00	5 semanas	Elaboración de Política de uso de controles criptográficos para el envío de información sensible.	Documento: Política de Uso de Controles Criptográficos.
Bitácora de Trabajos	Destrucción de registros.	Uso incorrecto del aplicativo	MITIGAR A.12.1.1	Dep. Tecnología	Personas. Tiempo.	$0.00	5 semanas	Documentación de procedimientos operaciones / manuales de usuario de aplicativos y registros.	Documentos: Procedimientos operacionales y Manuales de Uso.
Bitácora de Trabajos	Cambio involuntario de datos	Falta de manual de usuario							
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Almacenamiento en la Nube / Software de Simulación de Ingeniería	Cambio involuntario de datos	Falta de manual de usuario							
Contrato de Obra / Presupuesto Referencial / Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Acta de Reunión / Informe Final de Etapa de Detalle	Incumplimiento de normas y reglas	Ausencia de documentación							
Equipos Celulares	Fuga de información	Falta de control del uso del dispositivo	MITIGAR A.6.2.1	Dep. Tecnología	Personas. Tiempo.	$0.00	2 semanas	Elaboración de Política interna para uso de	Documento: Política de Uso de Dispositivos Móviles.

Equipos Celulares	Desastre de origen humano	Manipulación inadecuada del dispositivo						dispositivos móviles	
Equipos Celulares	Perdida de Equipos	Inadecuado nivel de concienciación de los empleados sobre el uso del dispositivo							
Planos de Diseño / Informe de Novedades de Etapa de Detalle / Documento de Trazabilidad / Informe Final de Etapa de Detalle / Software de Simulación de Ingeniería	Cambios no autorizados de registros.	Falta de conocimiento del rol	MITIGAR A.7.1.2	Dep. Recursos Humanos	Personas. Tiempo.	$0.00	2 semanas	Actualización de contratos con términos y condiciones que incluyan la Seguridad de la Información.	Socialización: Contratos persona a persona.
Documento de Trazabilidad	Daño causado por terceros.	Contraseñas inseguras.	MITIGAR A.9.4.3	Dep. Tecnología	Personas. Tiempo.	$0.00	1 semana	Elaboración de propuesta para el Sistema de Gestión de Contraseñas.	Propuesta: Sistema de Gestión de Contraseñas.
Equipos Celulares	Errores de mantenimiento	Mantenimiento insuficiente	TRANSFERIR A.11.2.4	Dep. Tecnología	Personas. Tiempo. Dinero.	$800.00	5 semanas	Levantamiento de propuestas para mantenimientos de equipo. Valor asignado semestral.	Propuesta: Mantenimiento de Equipos.
Almacenamiento en la Nube	Errores de Software	Sincronización inadecuada de los archivos	ACEPTAR Se acepta el riesgo ya que el Software para Almacenamiento en la Nube es responsabilidad del proveedor						

Fuente: Los Autores

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se conoce que, al término de este Trabajo de Titulación, la empresa JK Ingeniería no ha optado aun por la obtención de la certificación 27001; sin embargo, con la Gestión de Riesgos realizada sobre uno de sus mayores procesos críticos le deja la experiencia y conocimientos necesarios para continuar con la ruta trazada en Gestión de Seguridad de la Información.

2. El inventario de activos realizado ha recopilado activos de información críticos para la continuidad del proceso de Fiscalización, varios de ellos aun conteniendo información similar, presentan amenazas/vulnerabilidades diferentes debido a su exposición o

manejo particular, por lo que cada uno ha sido evaluado por separado con el fin de tratar acertadamente a cada riesgo resultante.

3. Los controles que han sido aplicados están atados a las vulnerabilidades encontradas. Asimismo, se busca que estos controles estén embebidos dentro de los procesos como parte de la respuesta a los riesgos para proteger la confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

1. Poner en funcionamiento, dentro de los tiempos establecidos, el plan de tratamiento de riesgos elaborado.

2. Continuar con la evaluación de los activos de información del resto de procesos presentes en la actividad de la Empresa ya que prevenir es mejor que corregir.

3. Identificar los Riesgos Positivos dentro del proceso de Fiscalización e incluirlos en la Matriz de Riesgos; es decir aquellos riesgos que generen valor al proceso y permitan mejorar o explotar oportunidades.

4. Planificar auditorías internas que permitan recoger actualizaciones del estado actual de los controles. Las auditorias permitirán verificar si los controles aplicados han mitigado correctamente las vulnerabilidades.

BIBLIOGRAFIA

[1] Asamblea Nacional Constituyente, Constitución de la Republica del Ecuador, 2008

[2] Asamblea Nacional Constituyente, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009

[3] López, A., Serie 27K. [online] Iso27000.es. Available at: <http://www.iso27000.es/iso27000.html> [Accessed 06 March 2019].

[4] ISACA, "Un Marco De Negocio Para El Gobierno Y La Gestión De Las TI De La Empresa". [e-book] Capítulo de Madrid de ISACA. Available at: <http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf> [Accessed 4 November 2019].

[5] Chaplin, M., & Creasey, J., "The 2011 Standard of Good Practices for Information Security", Information Security Forum Limited, 2011

[6] International Organization for Standardization, "Information security management systems - overview and vocabulary" (ISO/IEC 27000:2013). Geneva: ISO, 2013.

[7] Office of the Government Chief Information Officer, "An Overview of ISO/IEC 27000 family of Information Security Management System Standards", 2015

[8] International Organization for Standardization, "Risk management - principles and guidelines" (ISO 31000). Geneva: ISO, 2009.

[9] International Organization for Standarization, "Tecnología de información. Técnicas de seguridad. Gestión del Riesgo de la Seguridad de la Información" (ISO/IEC 27005:2018). Geneva: ISO, 2018.

[10] A. Ramírez & Z. Ortiz, "Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios", Ingeniería, vol. 16, no. 2, pp. 56-66, 2011.

[11] "PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", Administracionelectronica.gob.es. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Accessed: 04- Apr- 2019].

[12] H. Alemán Novoa & C. Rodríguez Barrera, “Metodologías para el análisis de riesgos en los sgsi”, Publicaciones E Investigación, vol. 9, pp. 73 - 86, oct. 2015.

[13] A. Abril Estupiñán, J. Pulido, & J. Bohada Jaime, “Análisis de riesgos en seguridad de la información”, Ciencia, Innovación y Tecnología (*RCIYT)*, vol. 1, pp. 40-53, nov. 2013.

[14] G. Stoneburner, A. Goguen, & A. Feringa, "Risk Management Guide for Information Technology Systems", National Institute of Standards and Technology (NIST), 2002

[15] Cloudcorp IT Consulting, "La Gestión en la seguridad de la información según ITIL, Cobit e ISO 27000", Cloudcorp.com.ec. [Online]. Available: https://www.cloudcorp.com.ec/estandares-de-si. [Accessed: 04- Nov- 2019].

[16] ISOTools Excellence, "¿Cuál es la terminología que utiliza la nueva ISO 31000?", Software ISO, 2018. [Online]. Available: https://www.isotools.org/2018/02/28/la-terminologia-utiliza-la-nueva-iso-31000. [Accessed: 11- Feb- 2019].

[17] E. Kowask, F. Alcantara, A. Motta & J. Piccolini, "Gestión del Riesgo de las TI NTC 27005", RENATA - Universidad Nacional de Colombia - Facultad de Ingeniería, 2014

[18] International Organization for Standarization, “Information technology — Security techniques — Code of practice for information security controls” (ISO/IEC 27002:2013). Geneva: ISO, 2013