



PLAN DE GESTIÓN DE RIESGO

Versión 1.0

04/01/2023

INTEGRANTES:

- Jessica Toro (6806)
- Homero Ojeda (6834)
- Michael Paucar (6581)
- Rubén Valencia (6795)
- Gabriel Cáceres (6742)
- Anderson Santana (6796)

HISTORIAL DE VERSIONES

FECHA	VERSIÓN	AUTOR	ORGANIZACIÓN	DESCRIPCIÓN
26/12/2022	0	Homero Ojeda	ThunderTeam	Se descargó el modelo de plantilla.
28/12/2022	0.1	Jessica Toro	ThunderTeam	Se empezó a trabajar en la sección 1 y revisión completa del documento
03/12/2023	0.2	Rubén Valencia	ThuderTeam	Se empezó a trabajar en la sección 2.1
04/01/2023	1.0	Michael Paucar	ThunderTeam	Se empezó a trabajar en la sección 2.2 – 2.4
04/01/2023	1.0	Anderson Santana	ThunderTeam	Se empezó a trabajar en la sección 3
04/01/2023	1.0	Gabriel Cáceres	ThunderTeam	Se empezó a trabajar en la sección 2.5 – 2.7

Contenido

1	INTRODUCCIÓN	4
1.1	Propósito del Plan de Gestión de Riesgos	4
2	PROCEDIMIENTO DE GESTIÓN DE RIESGOS	4
2.1	Proceso	4
2.2	Identificación de riesgos.....	6
2.3	Análisis de riesgos	7
2.4	Análisis cualitativo de riesgos	12
2.5	Análisis de Riesgo Cuantitativo	13
2.6	Planificación de la respuesta al riesgo	16
2.7	Seguimiento, control y notificación de riesgos	17
3	HERRAMIENTAS Y PRÁCTICAS	18
3.1	APROBACIÓN DEL PLAN DE GESTIÓN DE RIESGOS	18

1 INTRODUCCIÓN

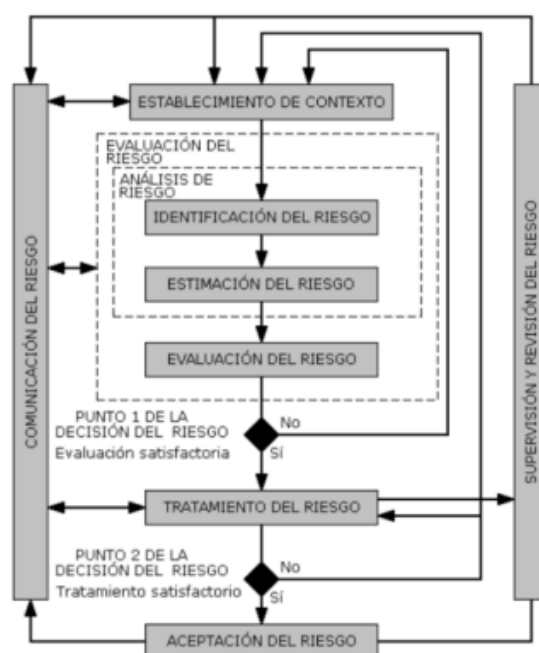
1.1 Propósito del Plan de Gestión de Riesgos

El objetivo de definir un Plan de Gestión de Riesgos del proyecto Policy Managment equipo Thunderteam , en el que se desarrollará una ruta a seguir con un plan que permita reducir o eliminar el impacto de los riesgos durante el desarrollo del proyecto. Para la gestión de riesgos se ha tomado como referencia la guía del PMBOK en la cual establece la identificación, evaluación, plan de respuesta a riesgos, seguimiento y control, secuenciales e iterativos. Los cuales aseguran efectividad del plan de gestión de riesgos sobre el proyecto en cuestión, para poder identificar los posibles riesgos que se pueden presentar, de igual forma categorizarlos evidenciando su probabilidad de ocurrencia e impacto en el proyecto y al final proponer unas estrategias de mitigación del riesgo en caso de llegar a materializarse con el fin de asegurar que el desarrollo del proyecto cumple con una adecuada planeación, en la cual se pueden prever los posibles riesgos que pueden generar alteraciones durante la ejecución de la aplicación. Con los riesgos existentes hoy en día en cada uno de los proyectos desarrollados a nivel software, se evidencia la necesidad de desarrollar métodos que permitan identificar la probabilidad de ocurrencia e impacto de un evento atípico, facilitando el control de estos en el caso de que se presenten en las diferentes etapas de desarrollo.

2 PROCEDIMIENTO DE GESTIÓN DE RIESGOS

2.1 Proceso

En el proceso de gestionar un riesgo tomamos que el gerente de proyecto Ing. Saul Ibarra y todo el equipo de trabajo Thunderteam, se asegura que el proceso de identificación de cualquier riesgo se logrará mitigar lo más antes posible por tal razón de describe a continuación las pautas técnicas donde el director será el administrador de riesgo para este proyecto.



A continuación, se muestra las actividades para gestionar los riesgos que existirán durante y después de la implementación del proyecto.

PROCESO PARA LA GESTIÓN DE RIESGOS

ACTIVIDADES	PASOS
<i>Establecimiento del contexto</i>	1. Consideraciones Generales - Levantamiento de información inicial
	2. Establecer criterios básicos para la Gestión del Riesgo
	3. Definir alcance y límites de la Gestión del Riesgo
	4. Establecer una organización para la operación del SGRSI
<i>Valoración del Riesgos</i>	5. Identificar Activos de Información
	6. Identificar las amenazas y las vulnerabilidades
	7. Identificar los controles existentes
	8. Identificar consecuencias
	9. Valorar las consecuencias
	10. Valorar los incidentes
	11. Determinar el nivel de estimación del riesgo
	12. Evaluar el riesgo
<i>Tratamiento del Riesgo</i>	13. Selección de controles de mitigación
<i>Aceptación del Riesgo</i>	14. Aceptación de los riesgos
<i>Comunicación del Riesgo</i>	15. Comunicación de los riesgos encontrados

2.2 Identificación de riesgos

En el proceso de desarrollo de este proyecto el equipo de desarrollo tomo la decisión de que pueda ser medido a través de la metodología OSWAP para la evaluación de riesgos por lo tanto se realizó un listado con los problemas más comunes en el proceso de desarrollo antes y después de este, que muy a grandes rasgos, define el Riesgo potencial como el producto entre la probabilidad de ocurrencia o explotación de una vulnerabilidad y el Impacto de un ataque exitoso, considerando siempre las variables de impacto tecnológico e impacto en el negocio, así como la facilidad de detección, explotación y prevalencia de la vulnerabilidad

No.	RIESGO	NIVEL			DESCRIPCIÓN
		A	M	B	
RG1	<i>Inyección</i>				Los parámetros de entrada mal gestionados, dentro de la programación, pueden provocar una vulnerabilidad que permita a un hacker inyectar información en una base de datos o a un intérprete
RG2	<i>Pérdida de autenticación y gestión de sesiones</i>				Cuando las claves no se protegen convenientemente, un atacante puede aprovechar vulnerabilidades para entrar y robar la información sensible.
RG 3	<i>Datos sensibles accesibles</i>				Es importante que las transacciones sean PCI compliance (Payment Card Industry Compliance) o en español "Cumplimiento de la industria de tarjetas de pago", unos estándares de seguridad para proteger los datos de los dueños de tarjetas de crédito durante, y después, de una transacción online
RG 4	<i>Entidad externa de XML (XXE)</i>				Las inyecciones de entidades externas son un tipo de ataque contra una aplicación que analiza las entradas XML y se combaten con software

			que no use parsers (analizadores de sintaxis externos).
RG 5	<i>Control de acceso inseguro</i>		Los atacantes utilizan herramientas SAST y DAST para detectar vulnerabilidades en el acceso, ya sean por medios manuales o automáticos.
RG 6	<i>Configuración de seguridad incorrecta</i>		Aunque esta configuración se aplica a lo anteriormente visto, sobre todo a la exposición de datos y a la protección de usuarios
RG 7	<i>Cross site scripting (XSS)</i>		XSS es un vector de ataque que los hackers utilizan para robar información, hacerse con las sesiones de los usuarios y poner en riesgo el navegador, dejando vulnerable la integridad del sistema.
RG 8	<i>Decodificación insegura</i>		La deserialización o también llamada decodificación, debe ser segura, ya que puede ocasionar la ejecución de código malicioso. Afecta a todo el WordPress, cachés, BBDD y tokens de APIs.
RG 9	<i>Componentes con vulnerabilidades</i>		Es un problema muy extendido y es posible que los equipos de desarrollo ni siquiera entiendan qué componentes usan en su aplicación o API, por lo que determinar las vulnerabilidades requiere un esfuerzo añadido
RG 10	<i>Insuficiente monitorización y registro</i>		El registro y monitoreo insuficiente de cualquier sistema, proporciona múltiples puertas traseras e infracciones que pueden ser difíciles de identificar y resolver si no existe un seguimiento eficaz.

2.3 Análisis de riesgos

Para este apartado el equipo de desarrollo Thunderteam indico algunas soluciones previas al analizar los riesgos que podría presentar nuestro proyecto tomando como referencia la metodología OSWAP para la gestión de riesgos, con el análisis de todos estos elementos y con la

guía metodológica que se presenta a continuación, es posible, con bastante asertividad, definir el real nivel de riesgo expuesto y a partir de su identificación tomar las medidas para erradicarlo en el mejor caso, o mitigarlo para reducir los potenciales efectos de una explotación

ID RIESGO	NIVEL			POSIBLES SOLUCIONES
	A	M	B	
RG1				<ul style="list-style-type: none"> • Contraseñas robustas • Versiones seguras • Plugins seguros, actualizados, compatibles y originales • Temas seguros y originales • Usuarios y prefijos de las BBDD que no sean por defecto • Moderación de los comentarios y un complemento que evite SPAM (Akismet) • Un hosting que tenga buenos sistemas de seguridad. • Hosting con versiones seguras de software y WAF (Web Application Firewall). • Permisos en archivos sensibles.
RG2				<ul style="list-style-type: none"> • Definir las secret_keys • Ocultar los errores de login • Utilizar únicamente dos administradores • Usar Doble verificación
RG3				<ul style="list-style-type: none"> • RGPD (Reglamento General de Protección de Datos) • Hosting RGPD y PCI compliance • Gestionar permisos de los usuarios • Eliminación de datos sensibles • SSL = HTTPS
RG4				<ul style="list-style-type: none"> • Software original y reconocido • No incluir parser XML • No incluir parsers en PHP • No cargar extensiones externas (XMLWRITER, DOM, XMLREADER)
RG5				<ul style="list-style-type: none"> • Desactivar XML-RPC • Inspeccionar las llamadas de las APIs (JSON REST API) • Disponer de copias de seguridad
RG6				<ul style="list-style-type: none"> • Utilizar permisos para archivos y carpetas
RG7				Tener en cuenta validar todo:

		<ul style="list-style-type: none"> • is_numeric() • preg_match() • filter_var() • in_array() <p>Sanear todo:</p> <ul style="list-style-type: none"> • sanitize_email • sanitize_file_name • sanitize_html_class • sanitize_text_field • sanitize_textarea_field • esc_url_raw • sanitize_option • sanitize_meta • wp_kses • sanitize_key • sanitize_user • sanitize_mime_type • sanitize_title • wp_filter_post_kses <p>Escapa todo:</p> <ul style="list-style-type: none"> • esc_html • esc_url • esc_js • esc_attr • esc_textarea
RG 8		<ul style="list-style-type: none"> • Mantener el CMS actualizado • Implementar controles de integridad como firmas digitales en cualquier objeto serializado
RG 9		<ul style="list-style-type: none"> • No alojarse en hostings no seguros • No utilizar software con vulnerabilidades conocidas o que han sido discontinuados.
RG 10		<ul style="list-style-type: none"> • Código ofuscado • Código base64

			<ul style="list-style-type: none"> • Llamadas al sistema (exec, passthru, system, shell_exec, etc.) • Ejecuciones de código PHP (eval, assert, preg_replace, etc.) • Exposiciones de información (phpinfo, getenv, getmygid/pid/uid, etc.) • Funciones del sistema de archivos (fopen, bz/gzopen, chgrp/own/mod, etc.) • RGPD (plugin)
--	--	--	---

Además, debemos tomar en cuenta la identificación de que activos están comprometidos con los riesgos antes mencionados entre otros como:

- Hardware.
- Software.
- Red.
- Personal.
- Ubicación.
- Estructura de la organización

Donde se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización

NO. ACTIVO	SUBPROCESO	TIPO ACTIVO	NOMBRE ACTIVO	ID_RIESGO	UBICACIÓN
AC1	APLICACIONES INFORMÁTICAS	Software de aplicación	Propietario desarrollo por la organización	RG 10	Edificio Central
AC2		Software de aplicación	Cliente	RG 02	Edificio Central
AC4		Software de aplicación	Gestión de la información	RG 06	Data Center
AC5		Software de aplicación	Herramientas de bases de datos	RG 01	Data Center
AC6		Software de aplicación	Middleware	RG 05	Data Center
AC7		Sistemas operativos	Servidores	RG 08 RG 07 RG 03 RG-04	Data Center
AC8		Sistemas operativos	Dispositivos de red	RG 10	Edificio Central
AC9		Sistemas operativos	Ordenadores de sobremesa	RG 09	Edificio Central
AC10		Sistemas operativos	Dispositivos de mano e incrustados	RG 04	Edificio Central
AC11		Servicios de TI	Enlaces	RG 10	Edificio Central
AC12		Servicios de TI	Administración de procesos	RG 10	Edificio Central
AC13		Servicios de TI	Anti-spam	RG 10	Edificio Central
AC14		Servicios de TI	Mantenimiento de software	RG 10	Edificio Central
AC15		Servicios de TI	Servicios de autenticación de usuario	RG 10	Edificio Central
AC16		Servicios de TI	Administración de procesos	RG 10	Edificio Central

AC17	TALENTO HUMANO	Personal	Trabajadores temporales	RG 04	Edificio Central
AC18		Personal	Consultores externos	RG 04	Edificio Central
AC19		Personal	Asesores especialistas	RG 04	Edificio Central
AC20		Personal	Contratistas especializados	RG 05	Edificio Central
AC21		Personal	Proveedores	RG 05	Edificio Central
AC22		Personal	Socios	RG 05	Edificio Central
AC23		Personal	Equipo de desarrollo	RG 02	Edificio Central
AC24		Personal	Auxiliares de desarrollo	RG 08	Edificio Central

2.4 Análisis cualitativo de riesgos


La ponderación de activos es una etapa en la que participan las unidades del negocio involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos.

Esta ponderación fue realizada en términos de “alto, medio o bajo” donde se asigna un valor cuantitativo a cada valor cualitativo




A continuación, se presentan las referencias para la valoración del impacto en los activos de la información.

- VALORACIÓN DEL IMPACTO EN TÉRMINOS DE LA PERDIDA DE LA CONFIDENCIALIDAD**




CONFIDENCIALIDAD	PUN	ASIG	CRITERIO
ALTO	3		La divulgación no autorizada de la información tiene un efecto crítico
MEDIO	2		La divulgación no autorizada de la información tiene un efecto limitado

BAJO	1		<i>La divulgación de la información no tiene ningún efecto</i>
------	---	---	--

- **VALORACIÓN DEL IMPACTO EN TÉRMINOS DE LA PERDIDA DE LA INTEGRIDAD**

INTEGRIDAD	PUN	ASIG	CRITERIO
ALTO	3		<i>La destrucción o modificación no autorizada de la información tiene un efecto severo</i>
MEDIO	2		<i>La destrucción o modificación no autorizada de la información tiene un efecto considerable</i>
BAJO	1		<i>La destrucción o modificación de la información tiene un efecto leve</i>

- **VALORACIÓN DEL IMPACTO EN TÉRMINOS DE LA PÉRDIDA DE LA DISPONIBILIDAD**

DISPONIBILIDAD	PUN	ASIG	CRITERIO
ALTO	3		<i>La interrupción al acceso de la información o los sistemas tienen un efecto severo</i>
MEDIO	2		<i>La interrupción al acceso de la información o los sistemas tienen un efecto considerable</i>
BAJO	1		<i>interrupción al acceso de la información o los sistemas tienen un efecto mínimo</i>

2.5 *Análisis de Riesgo Cuantitativo*

Para llevar a cabo una gestión efectiva de la seguridad de procesos, es necesario tanto tener ciertos datos iniciales de entrada para poder realizar el análisis cuantitativo de riesgos en el proyecto.

A) Entradas

- Registro de Riesgos: Algunos elementos clave del registro de Riesgos para el Análisis Cuantitativo de Riesgos incluyen la lista de Riesgos identificados, la lista

de prioridades o clasificaciones relativas de los Riesgos del Proyecto y los Riesgos agrupados por categorías

- Plan de Gestión de Riesgos: Algunos elementos del Plan de Gestión de Riesgos son clave para el Análisis Cuantitativo de Riesgos, por ejemplo, los roles y responsabilidades de la Gestión de Riesgos, asignaciones presupuestarias y actividades del cronograma destinados a la Gestión de Riesgos, categorías de Riesgo, la RBS y las tolerancias al Riesgo por parte de los interesados en el Proyecto.
- Planes de Gestión de Costos y del Cronograma: El plan de Gestión de costes del Proyecto establece el formato y los criterios para planificar, estructurar, estimar, preparar el presupuesto y controlar los costes del Proyecto, incluidas las asignaciones a la Gestión de Riesgos. El plan de Gestión del cronograma del Proyecto establece el formato y los criterios para desarrollar y controlar el cronograma del Proyecto, incluidas las acciones de Gestión de Riesgos.

B) Técnicas o herramientas

- Técnicas de Recopilación y Representación de Datos: Entrevistas y reuniones. Distribuciones de probabilidad. Juicio de expertos
- Técnicas de Análisis Cuantitativo de Riesgos y de Modelado:
 - Análisis de sensibilidad. Ayuda a determinar qué riesgos tienen un mayor impacto potencial en el proyecto. Este método evalúa el grado en que la incertidumbre de cada elemento del proyecto afecta el objetivo que está siendo examinado, cuando todos los demás elementos inciertos se mantienen en sus valores de línea base.
 - Modelado y simulación. Una simulación de proyecto utiliza un modelo que traduce las incertidumbres detalladas especificadas del proyecto en su impacto potencial sobre los objetivos de este. Las simulaciones iterativas se realizan habitualmente utilizando la técnica Monte Carlo.

C) Salidas

- Actualizaciones a los documentos del Proyecto:
 - Análisis probabilístico del Proyecto
 - Probabilidad de alcanzar los objetivos de costo y tiempo
 - Lista priorizada de riesgos cuantificados
 - Tendencias en los resultados del análisis cuantitativo de riesgos

NO. ACTIVO	NOMBRE ACTIVO	TIPO ACTIVO	UBICACIÓN	VALORACIÓN DEL IMPACTO			
				C	I	D	TOTAL, VA
AC1	Propietario desarrollo por la organización	Software de aplicación	Edificio Central	1	2	1	1,3
AC2	Cliente	Software de aplicación	Edificio Central	2	2	1	1,7
AC4	Gestión de la información	Software de aplicación	Data Center	3	2	3	2,7
AC5	Herramientas de bases de datos	Software de aplicación	Data Center	2	3	2	2,3
AC6	Middleware	Software de aplicación	Data Center	1	2	2	1,7
AC7	Servidores	Sistemas operativos	Data Center	3	3	3	3,0
AC8	Dispositivos de red	Sistemas operativos	Edificio Central	1	1	2	1,3
AC9	Ordenadores de sobremesa	Sistemas operativos	Edificio Central	1	2	2	1,7
AC10	Dispositivos de mano e incrustados	Sistemas operativos	Edificio Central	2	2	2	2,0
AC11	Enlaces	Servicios de TI	Edificio Central	1	2	1	1,3
AC12	Administración de procesos	Servicios de TI	Edificio Central	2	3	2	2,3
AC13	Anti-spam	Servicios de TI	Edificio Central	1	2	1	1,3
AC14	Mantenimiento de software	Servicios de TI	Edificio Central	2	2	2	2,0
AC15	Servicios de autenticación de usuario	Servicios de TI	Edificio Central	3	3	3	3,0

AC16	Administración de procesos	Servicios de TI	Edificio Central	2	3	3	2,7
AC17	Trabajadores temporales	Personal	Edificio Central	2	2	2	2,0
AC18	Consultores externos	Personal	Edificio Central	2	2	2	2,0
AC19	Asesores especialistas	Personal	Edificio Central	2	1	2	1,7
AC20	Contratistas especializados	Personal	Edificio Central	2	2	1	1,7
AC21	Proveedores	Personal	Edificio Central	2	1	1	1,3
AC22	Socios	Personal	Edificio Central	1	2	2	1,7
AC23	Equipo de desarrollo	Personal	Edificio Central	2	2	2	2,0
AC24	Auxiliares de desarrollo	Personal	Edificio Central	2	2	1	1,7

2.6 Planificación de la respuesta al riesgo

Las respuestas a los riesgos planificadas deben ser congruentes con la importancia del Riesgo. Tener un coste efectivo en relación con el desafío. Ser aplicadas a su debido tiempo, ser realistas dentro del contexto del Proyecto.

No.	RIESGO	NIVEL			RESPUESTA
		A	M	B	
RG1	<i>Inyección</i>				Evitar
RG2	<i>Pérdida de autenticación y gestión de sesiones</i>				Evitar
RG 3	<i>Datos sensibles accesibles</i>				Evitar
RG 4	<i>Entidad externa de XML (XXE)</i>				Evitar

RG 5	<i>Control de acceso inseguro</i>				Mitigar
RG 6	<i>Configuración de seguridad incorrecta</i>				Mitigar
RG 7	<i>Cross site scripting (XSS)</i>				Mitigar
RG 8	<i>Decodificación insegura</i>				Mitigar
RG 9	<i>Componentes con vulnerabilidades</i>				Aceptar
RG 10	<i>Insuficiente monitorización y registro</i>				Transferir

Las respuestas al riesgo deben resultar en:

- Actualizaciones a los Documentos del Proyecto.
- Actualizaciones al Plan para la Dirección del Proyecto. El plan de Dirección del Proyecto se actualiza a medida que se añaden actividades de respuesta a los Riesgos.

2.7 Seguimiento, control y notificación de riesgos

Todas las actividades de análisis de riesgos presentadas hasta el momento tienen una sola meta: auxiliar al equipo del proyecto a desarrollar una estrategia para lidiar con el riesgo. Una estrategia efectiva debe considerar tres temas:

- Evitar el riesgo

Si un equipo de software adopta un enfoque proactivo ante el riesgo, evitarlo siempre es la mejor estrategia. Esto se logra desarrollando un plan para mitigación del riesgo.

- Monitorear el riesgo


Conforme avanza el proyecto, comienzan las actividades de monitoreo de riesgos. El gerente de proyecto monitorea factores que pueden proporcionar un indicio de si el riesgo se vuelve más o menos probable

- Manejar el riesgo y planificar la contingencia.

El manejo del riesgo y la planificación de contingencia suponen que los esfuerzos de mitigación fracasaron y que el riesgo se convirtió en realidad

3 HERRAMIENTAS Y PRÁCTICAS

3.1 APROBACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Nombre / Cargo	Fecha	Firma
Ing. Abelardo Navarrete/ Administrador de Contrato		
Ing. Saúl Ibarra/ Gerente de Proyecto		