FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROBLEMÁTICAS Y RIESGOS DE UN PROYECTO

Docente: Mg. Evelyn Ayala

INDICE

UCV
UNIVERSIDAD CÉSAR VALLEJO

01

INTRODUCCIÓN

GESTIÓN DE PROYECTOS

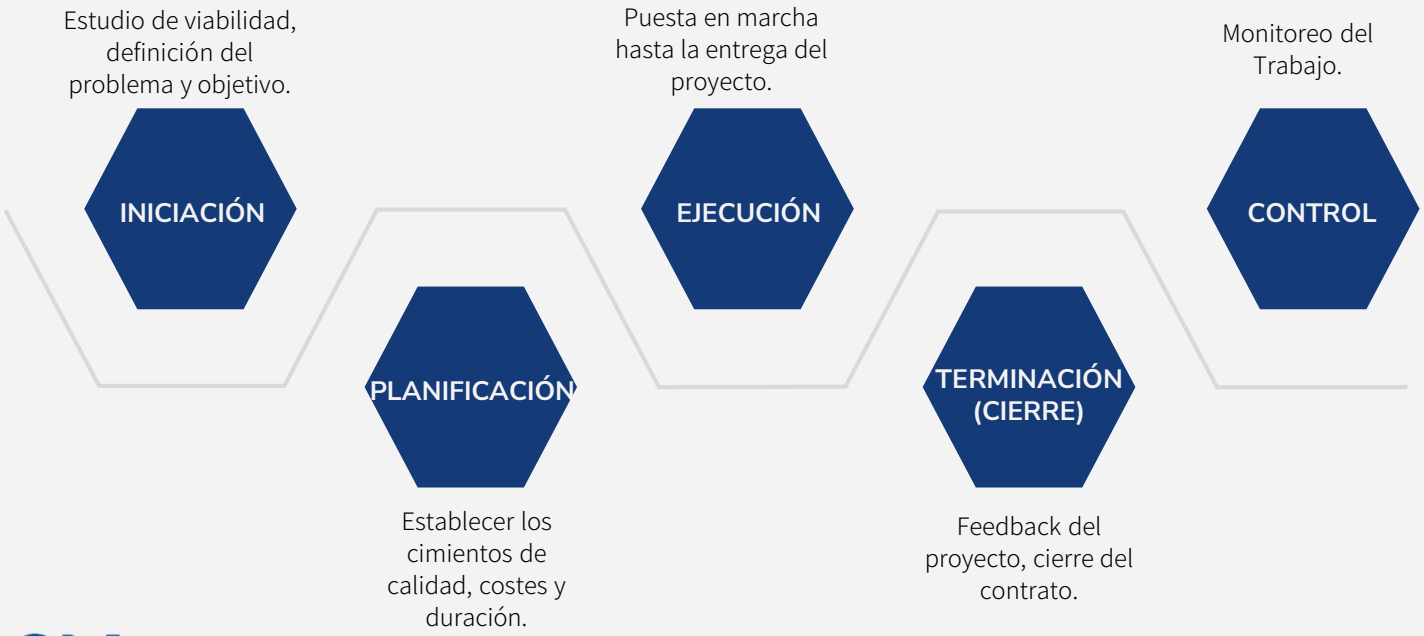
Es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo.

Project Management Institute.

UCV UNIVERSIDAD CÉSAR VALLEJO

PMI Project Management Ready

ETAPAS DE LA GESTIÓN DE PROYECTOS



UCV
UNIVERSIDAD CÉSAR VALLEJO

ÁREAS DE CONOCIMIENTO

UCV
UNIVERSIDAD
CÉSAR VALLEJO

Los problemas o riesgos no gestionados pueden generar **retrasos, sobrecostos, déficit en el desempeño o pérdida de reputación**.

Las oportunidades aprovechadas pueden conducir a beneficios como **reducción de tiempo y costo, mejora en el desempeño y buena reputación**.

UCV
UNIVERSIDAD CÉSAR VALLEJO

02

PROBLEMÁTICAS Y RIESGOS DE UN PROYECTO

CONSIDERACIONES PREVIAS

UCV
UNIVERSIDAD CÉSAR VALLEJO

OBJETIVOS DE LA GESTIÓN DE RIESGOS

- Aumentar la probabilidad y/o el impacto de los riesgos positivos.
- Disminuir la probabilidad y/o el impacto de los riesgos negativos.

A fin de optimizar las posibilidades de éxito del proyecto.

03

PROCESOS DE LA GESTIÓN DE LOS RIESGOS

UCV
UNIVERSIDAD
CÉSAR VALLEJO

PROCESOS DE GESTIÓN DE LOS RIESGOS DEL PROYECTO

PLANIFICAR LA GESTIÓN DE LOS RIESGOS

Se define cómo realizar las actividades de gestión de riesgos de un proyecto.
En base a documentos en base al proyecto y a la empresa en sí.

Ejemplo:

Etapa	ID	Actividad	R	A	C	I	Sesión	Predecesora	SLA de Seguridad	SLA Proyecto
1. Alcance – contexto y criterio	1	1.1. Alcance y limitaciones.	ASI	RDP	RDP	RDP	1		2 dias	
	2	1.2. Determinación el contexto.	ASI	RDP	RDP	RDP	1			
	3	1.3. Criterios de evaluación del riesgo.	ASI	RDP	RDP	RDP	1			
	4	Entrega de contexto del proyecto, acuerdos y checklist parcialmente completo	ASI	RDP	RDP	RDP	1			
	5	Entrega de Checklist de Requerimientos Completo, con fechas de implementación o evidencias previas.	RDP	ASI	ASI	ASI				10 dias
2. Identificación del riesgo	6	2.1. Identificación de los activos.	RDP							
	7	2.2. Identificación de fuentes de riesgo.	ASI							
	8	2.3. Identificación de las amenazas.	ASI							
	9	2.4. Identificación de los controles.	ASI	ASTI	RDP	RDP				
	10	2.5. Identificación de las vulnerabilidades.	ASTI	ASI	RDP	ASI			10 dias	
	11	Informe de Vulnerabilidades tecnicas y fuentes de Riesgos								
3. Análisis del riesgo	12	Valoración de probabilidad de la amenaza.	ASI						5 dias	
	13	Valoración del impacto de materializarse la amenaza.	ASI							
4. Evaluación del riesgo	14	Valoración del riesgo.	ASI							
	15	Identificación de riesgos críticos.	ASI							
	16	Riesgo inherente.	ASI							
5. Tratamiento del Riesgo	17	Selección de controles.	ASI							
	18	Evaluación de riesgo residual.	ASI							
6. Aceptación del riesgo	19	Aceptación del plan de tratamiento.	RDP	ASI	ASI	ASI			2 dias	
	20	Aceptación del riesgo residual.	RDP	ASI	ASI	ASI				
7. Consulta y comunicación	22	Consulta y comunicación.	ASI						Durante todo el proceso	
8. Registro e informes	23	8.1. Registrar el riesgo.	ASI	RDP	RDP	RDP			2 dias	
	24	8.2. Control del registro.	ASI	RDP	RDP	RDP				
	25	8.3. Informes del riesgo.	ASI	RDP	RDP	RDP				
	26	8.4. Documentación de la gestión de riesgos.	ASI	RDP	RDP	RDP				
9. Seguimiento y revisión	27	9.1. Seguimiento y revisión.	ASI	RDP	RDP	RDP				

UCV
UNIVERSIDAD CÉSAR VALLEJO

Analista de Seguridad de la Información		ASI
Analista de Seguridad Tecnologica		ASTI
Respoonsable del Proyecto		RDP

- **R**esponsible (Responsable)
- **A**ccountable (Autoridad)
- **C**onsulted (Consultor)
- **I**nformed (Informado)

IDENTIFICAR LOS RIESGOS

Analizar qué riesgos pueden aparecer en relación al proyecto.

Objetivo de control ISO 27000		Riesgo Asocioado
A.13	Seguridad de las comunicaciones	**Exposición, alteración e indisponibilidad de la información,** debido a la falta de aplicación de mecanismos de bloqueo de ataques perimetrales
		Acceso no autorizado,debido a la exposición de puertos innecesario
		Exposición, alteración de la información, debido a la falta de aplicación de las 5 cabeceras de seguridad HTTP

Objetivo de control ISO 27000		Riesgo Asocioado
A.7	Gestión de accesos	**Acceso no autorizado** debido a la falta de un prceso de Gestión de Identidades, autenticación y control de acceso formal
		Acceso no autorizado debido a la ausencia de doble factor de autenticación
		Acceso no autorizado debido a la ausencia de mecanismos de autenticación robusta.

UCV
UNIVERSIDAD CÉSAR VALLEJO

REALIZAR EL ANÁLISIS CUALITATIVO DE RIESGOS

Se prioriza los riesgos del proyecto evaluando la probabilidad de ocurrencia y su impacto.

Ejemplo:

			Probabilidad				
			Muy bajo	Bajo	Moderado	Alto	Muy alto
			1	2	3	4	5
Impacto	Muy alto	5	5	10	15	20	25
	Alto	4	4	8	12	16	20
	Moderado	3	3	6	9	12	15
	Bajo	2	2	4	6	8	10
	Muy Bajo	1	1	2	3	4	5

Magnitud del Riesgo		Respuesta al Riesgo
<=25	**Critico**	Riesgo crítico se debe reducir el riesgo, evitar, compartir o transferir.
12 al 15	**Alto**	Riesgo importante se debe reducir el riesgo, evitar, compartir o transferir.
5 al 11	**Medio**	Riesgo moderado se debe reducir o asumir el riesgo acorde con lo que estipule la Alta Dirección.
<=4	**Bajo**	Riesgo tolerable se debe asumir el riesgo o gestionar mediante procedimientos de rutina, acorde con lo que estipule la Alta Dirección.

UCV
UNIVERSIDAD
CÉSAR VALLEJO

REALIZAR EL ANÁLISIS CUANTITATIVO DE RIESGOS

Se analiza numéricamente el efecto de los riesgos sobre los objetivos generales del proyecto.

Ejemplo:

Criticidad del Proyecto

Sensibilidad - ¿ El proyecto comteplad la siguiente información : ?	
1	No cuenta con información sensible, personal, financiera, Solamente es información publica.
2	Maneja datos personales, como datos que pemitan identificar a usuario (Nombre, DNI,Correo , numero, placa del vehiculo, entre otros)
3	Maneja información sensible y financieros, el impacto podria causar multas o sanciones regulatorias.
Exposicion	
1	No esta expuesto a internet , es un sistema interno de la compañía y no maneja datos sensibles, financieros.
2	Exposición de datoa sensible internmento en la compñaia, mediante un aplicativo interno interalacionado con los sistemas de informació Core dell negocio
3	Expuesto totalmente a internet sin restricciones, mediante una pagina web o interconexiones con terceros, asi como twambien integraciones directas a las bases de datos
Impacto en el negocio (	
1	No impacta en los objetivos estrategicos del negocio
2	Impacta parcialmente en los objetivos estrategicos del negocio
3	Impacta totalmente en los objetivos del negocio

Nivel de Riesgo		Descripción
Riesgo Critico	10 al 12	Requiere un Ethical Hacking + Vulnerabilidades + analisis de Riesgos
Riesgo Alto	6 al 9	Requiere un Ethical Hacking + Analisis de Riesgos.
Riesgo Medio	4 al 5	Requiere un analisis de vulnerabilidades Analisis de Riesgos
Riesgo Bajo	1 al 3	Requiere solamente visto bueno de seguridad

Impacto			Valoración		
Sensibilidad	Exposición	Impacto en el negocio	Calificación	Nivel de Criticidad	Opción de Tratamiento
3	3	3	9	ALTO	Requiere un Ethical Hacking + Analisis de Riesgos.

UCV
UNIVERSIDAD
CÉSAR VALLEJO

PLANIFICAR LA RESPUESTA A LOS RIESGOS

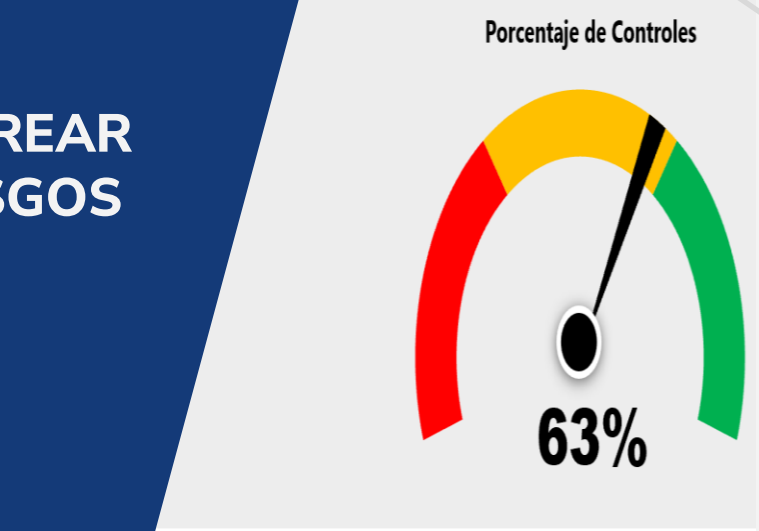
Se debe seleccionar estrategias y acordar acciones para abordar la exposición a los riesgos identificados.

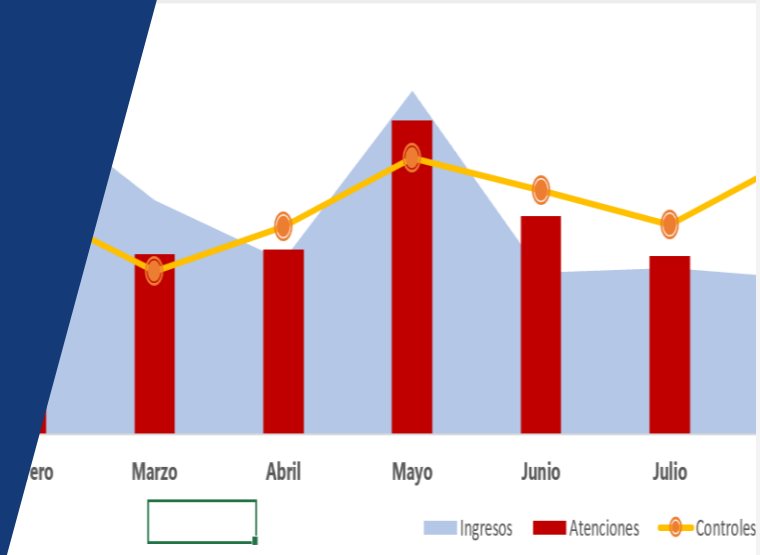
e control ISO 27000	Aplicabilidad	Codigo	Control	Detalles	Riesgo Asocioado
Gestión de accesos	SI	CA01	Se debe contar con un proceso de gestión de identidades , autenticación y control de acceso formal, a fin de garantizar el cumplimiento de altas, bajas y modificaciones de usuarios. Adicional el sistema debe contar con una matriz de Perfiles y Accesos	1.-La gestión de accesos en aplicaciones internas o para terceros (partners) debe estar a cargo del área de acceso de Seguridad de Información de tal forma que se garantize el cumplimiento de los procedimientos específicos de accesos 2.-En caso no aplique deben garantizar la gestión de credenciales de acuerdo a los estándares del área de accesos 3.-La aplicación debe prevenir el acceso a módulos o cuentas no permitidas por otros usuarios para evitar ataques de suplantación. 4.-Se debe crear una matriz detallada del acceso de cada usuario hacia los elementos del sistema.	Acceso no autorizado debido a la falta de un prceso de Gestión de Identidades, autenticación y control de acceso formal
	SI	CA02	El acceso de usuarios internos o terceros (partners) hacia aplicaciones expuestas en Internet debe contar con un segundo factor de autenticación que puede ser un certificado, un token digital, una dirección IP	1.-Los usuarios internos deben ingresar a aplicaciones expuestas en Internet mediante segundo factor de autenticación. La plataforma normalmente usada es el Azure AD 2.-Para el SFTP público el segundo factor puede ser un certificado o la dirección IP 3.-Para APIs publicadas para terceros el segundo factor es la IP que restringue el acceso mediante un ACL 4-Para el caso de accesos hacia APPs internas , el segundo factor es el app Intune instalado por RIMAC	Acceso no autorizado debido a la ausencia de doble factor de autenticación
	SI	CA03	La aplicación web o movil debe contar con mecanismos de autenticación que garantizen el uso de contraseñas robustas. Se recomienda la integración con el directorio activo en aplicaciones internas.	Se debe cumplir con los siguientes requisitos de passwords: 1.- Longitud mínima: 8 caracteres 2.- Debe incluir al menos un caracter en mayúscula. 3.- Debe incluir al menos un caracter en minúscula. 4.- Debe incluir al menos números 5.- Debe incluir un caracter especial. 6.- Debe forzar el cambio de la contraseña al primer ingreso o al haber restaurado una clave por defecto. 7.- No debe permitir el re-uso de las últimas 05 contraseñas 8.- Expiración de contraseñas.	Acceso no autorizado debido a la ausencia de mecanismos de autenticación robusta.

IMPLEMENTAR LA RESPUESTA A LOS RIESGOS

Implementar planes acordados de respuesta a los riesgos.

MONITOREAR LOS RIESGOS





Se debe hacer seguimiento a los riesgos identificados, identificar y analizar nuevos riesgos y evaluar la efectividad de la gestión de los riesgos a lo largo del proyecto.

ACTIVIDAD

En base a la empresa y al proyecto seleccionado, deberán realizar la Gestión de Riesgos.

Respecto a la gestión de problemas y riesgos del Proyecto:

- Identificar los riesgos.
- Realizar el análisis cualitativo de riesgos.
- Realizar el análisis cuantitativo de riesgos.
- Planificar la respuesta a los riesgos.
- Elaboración del dashboard o tablero de control (simulado)

MUCHAS GRACIAS

¿Preguntas?

UCV
UNIVERSIDAD CÉSAR VALLEJO