USO DE LA SEGURIDAD DE LA INFORMACIÓN EN LA DIRECCIÓN DE PROYECTOS

PROYECTO DE GRADO

Jennifer Coque Vásquez
Mara D. Kujundzic Riveros

Asesor
Ingrid L Muñoz
Msc Gestión Informática y Telecomunicaciones

FACULTAD DE INGENIERÍA
MAESTRÍA EN GERENCIA DE PROYECTOS
SANTIAGO DE CALI
2018

USO DE LA SEGURIDAD DE LA INFORMACIÓN EN LA DIRECCIÓN DE PROYECTOS

Jennifer Coque Vásquez
Mara D. Kujundzic Riveros

Trabajo de grado para optar al título de
Máster en Gestión de Proyectos y Tecnología con Énfasis en Ingeniería de Software

Asesor
Ingrid L Muñoz
Msc Gestión Informática y Telecomunicaciones

FACULTAD DE INGENIERÍA
MAESTRÍA EN GERENCIA DE PROYECTOS
SANTIAGO DE CALI
2018

Tabla de contenido

Pág.

Lista de tablas

Pág.

Lista de figuras

Pág.

Lista de gráficos

Pág.

Lista de anexos

Pág.

Resumen

La dirección de proyectos está enmarcada por un conjunto de procesos de estandarización, medición y control para garantizar las buenas prácticas, sin embargo, se identificó la carencia de políticas, procedimientos y controles que apoyen la disponibilidad, confidencialidad e integridad de la información en los grupos de procesos que manejan los proyectos bajo la metodología del PMBOK®. Por el contrario, en el estándar para la seguridad de la información, publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional en su versión más reciente ISO/IEC 27002:2013 busca garantizar que los riesgos de la seguridad de la información sean tenidos en cuenta durante todo el proyecto, tal como lo menciona en el numeral 6.1.5 Seguridad de la información en la gestión de proyectos.

Con la colaboración de empresas MiPymes en el sector de información y comunicaciones en la ciudad de Cali se identificaron las necesidades para proponer una nueva área de conocimiento dentro del marco PMBOK® encargada de gestionar la seguridad de la información, incluyendo procesos con entradas, herramientas y salidas en los grupos de procesos de inicio, planeación, ejecución, monitoreo y control, y cierre.

De igual forma, se deja abierta la posibilidad de buscar alternativas a esta propuesta, como podría ser analizar en qué área de trabajo ya existente dentro del marco del PMBOK® se podrían incluir nuevos procesos para la gestión de proyectos e incluso expandir el tema a otros marcos de trabajo para la dirección de proyectos.

Palabras clave: Seguridad de la información, proyectos, marco de trabajo proyectos, procesos, MiPymes, disponibilidad de la información, confidencialidad de la información, integridad de la información.

1. Introducción

1.1. Contexto y Antecedentes

El manejo de la información en un proyecto es un tema importante durante su desarrollo, ya que no solamente se debe garantizar que esté disponible para todos los miembros del equipo y los interesados, sino que a la vez se debe velar por su disponibilidad, integridad y confidencialidad debido al carácter estratégico que muchas veces tienen los proyectos en las compañías.

Dicho carácter estratégico hace que la documentación de un proyecto sea muy atractiva para la competencia o terceros interesados en hacer un uso inadecuado de la misma, ya que allí está el conocimiento, los conceptos, las ideas, la marcas, la información y los detalles de toda la arquitectura de redes y sistemas de la compañía (ISO/IEC 27002, 2013). De igual forma, la tecnología, así como ofrece grandes ventajas como los amplios alcances e impacto para la comunicación y volumen de almacenamiento, también es altamente vulnerable sin las medidas necesarias, ya que la información se puede perder, filtrar o corromper fácilmente.

A pesar de tener todo este peso para ser un factor crítico en la dirección de proyectos, la seguridad de la información no se referencia directamente en ninguna metodología, entiéndase Agile o cascada, o en los principales marcos de referencia, como es el caso del PMBOK®, PRINCE2, ISO 21500, entre otros.

Por el momento, la gestión del riesgo proporciona un terreno en el cual sus herramientas pueden usarse para proteger la documentación y los canales de comunicación, sin embargo, para muchos directores de proyectos incluir la seguridad de la información en la gestión de riesgos aún no es una práctica rigurosa, y muchas veces no se desarrolla con la profundidad requerida, ya sea por tiempo o alcance.

Ante esta situación en el 2013, la ISO/IEC 27001 en su Anexo A y la ISO/IEC 27002, buscan estandarizar el uso de la seguridad de la información en la gerencia de proyectos, en el numeral 6.1.5 se estipula que la seguridad de la información debe tenerse en cuenta en la dirección de proyectos, independientemente de la naturaleza del proyecto (ISO/IEC 27002, 2013). Así, describe unos lineamientos en los cuales la seguridad de la información se integra de forma más decisiva a la gerencia de proyectos. Algunos mencionados en el Anexo A son: (ISO/IEC 27001 Anexo A, 2013) (ISO/IEC 27002, 2013):

- Incluir los objetivos de la seguridad de la información en los objetivos del proyecto
- Llevar a cabo una evaluación de riesgos en las etapas tempranas del proyecto.
- Identificar los controles necesarios.
- La seguridad de la información debe hacer parte de todas las fases de la metodología aplicada del proyecto.

En este escenario, Domuz es una empresa que actualmente trabaja en proyectos y seguridad de la información, y con apoyo en su experiencia se plantea incluir procesos dentro del marco del PMBOK® que aumenten el éxito de proyectos al incluir procesos de Seguridad de la

Información, esto debido a que al identificar los riesgos asociados al manejo de la información e implementar controles que ayuden a cerrar la brecha, se lograría garantizar un buen manejo de la información a todos los interesados, lo cual es un soporte y respaldo al mitigar o evitar futuras materializaciones de riesgos asociados a la seguridad de la información.

Teniendo en cuenta que este marco agrupa 49 procesos en cinco grupos distribuidos en diez áreas de conocimiento, es posible proponer una nueva área del conocimiento, en la cual se relacionen herramientas, entradas y salidas relacionadas a la seguridad de la información y que sea transversal a todos los 5 grupos de procesos.

1.1 Planteamiento del Problema

El marco de buenas prácticas en gestión de proyectos otorgado por el PMBOK® mide el éxito de los proyectos controlando principalmente que se entregue lo que se ha previsto en el tiempo y costo acordado, además de cumplir con la calidad, el buen uso de recursos y la correcta gestión de riesgos.

Sin embargo, ninguno de los 49 procesos mencionados en la guía PMBOK® sexta edición del PMI® hace referencia a la seguridad de la información como buena práctica en la gestión de proyectos. La seguridad de la información con base en la ISO/IEC 27001 Anexo A y la ISO/IEC 27002 se refiere a la disponibilidad, confidencialidad e integridad de la información en organizaciones de cualquier tipo y tamaño, incluyendo todos los sectores. Conceptos que deben

estar integrados explícitamente desde la noción de un proyecto y como actividad en uno o varios de sus procesos (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013).

Aunque las políticas, estándares y procedimientos para la seguridad de la información en los proyectos no son ajenas para todas las empresas, son las Medianas, Pequeñas y Microempresas con menor conciencia de los riesgos que incurren al no tomar medidas de control. (MINTIC, 2016)

Por consiguiente, se considera necesario documentar un estudio acerca del manejo de la seguridad de la información durante la gestión de proyectos en las MiPymes (Medianas, Pequeñas y Micro empresas) en el sector Tecnologías de Información y Comunicaciones, con el fin de identificar y proponer las actividades que apoyen la disponibilidad, confidencialidad e integridad de la información durante la ejecución de los cinco grupos de procesos enmarcados por el PMBOK® mitigando los riesgos de seguridad de la información.

2. Objetivos

2.1 Objetivo General

Proponer procesos dentro de la dirección de proyectos que apoyen la disponibilidad, confidencialidad e integridad de la información durante el desarrollo de proyectos teniendo como base las necesidades de las MiPymes en el sector de información y comunicaciones en la ciudad de Cali.

2.2 Objetivos Específicos

1. Desarrollar una herramienta para determinar el manejo de la seguridad de la información durante la gestión de proyectos en las Micro, Pequeñas y Medianas empresas en el sector de información y comunicaciones en la ciudad de Cali.
2. Aplicar y analizar los resultados del sistema de medición diseñado, proporcionando información sobre el control en la disponibilidad, confidencialidad e integridad de la información durante la ejecución de proyectos en las MiPymes seleccionadas.
3. Proponer la inclusión de una nueva área del conocimiento para la Gestión de la seguridad de la información, con nuevos procesos que se deben tener en cuenta dentro de los grupos de procesos, que les permita a las organizaciones resguardar y proteger la información durante la ejecución de los proyectos.

3. Antecedentes

3.1 Marco Teórico

3.1.1 Dirección de proyectos en el marco según la Guía de los fundamentos para la dirección de Proyectos (PMBOK®) Sexta edición desarrollada por el PMI®.

De acuerdo al PMBOK®, un Proyecto es “un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único y se llevan a cabo para cumplir objetivos mediante la producción de entregables”. (Project Management Institute, 2017) Destacando como características (Muñoz, 2018):

- Tiene objetivos definidos
- Tiene un presupuesto
- Implica el uso temporal de recursos tanto humanos como materiales
- Tiene un inicio y un final bien definidos
- Tiene un cliente (quien recibe el resultado del proyecto, puede ser una persona, empresa o grupo)
- Impulsan el cambio
- Crea un producto, servicio o resultado único.
- Tiene un ciclo de vida, que puede ser predictivo, iterativo, incremental o adaptativo.

La Dirección de proyectos a su vez es definida como la aplicación del conocimiento, habilidades, herramientas y técnicas que se deben implementar para que las actividades de un proyecto logren cumplir con sus requisitos. Amarrado a esto, la dirección de proyectos es la responsable de evaluar y gestionar las restricciones que tiene un proyecto, las cuales son Tiempo, Alcance, Costo, Calidad, Riesgos y Recursos (Project Management Institute, 2017).

El marco que propone el PMBOK® para una dirección de proyectos efectiva incluye 49 procesos, que son divididos en 5 grupos y son distribuidos en 10 áreas de conocimiento de la siguiente forma (ver tablas 1 y 2):

Tabla 1. Descripción de las áreas de conocimiento y su interrelación con los grupos de proceso

Área de conocimiento	Descripción	Grupo de procesos con los que se entrelaza
Gestión de la Integración del Proyecto	Coordinar todos los elementos del proyecto	Inicio Planeación Ejecución Monitoreo y Control Cierre
Gestión del Alcance del Proyecto	Asegurar que se incluye todo, y solamente el trabajo requerido para el proyecto.	Planeación Monitoreo y Control
Gestión del Cronograma del proyecto	Asegurar la finalización a tiempo del proyecto.	Planeación Monitoreo y Control
Gestión de los Costos del proyecto	Asegurar el trabajo dentro del presupuesto aprobado	Planeación Monitoreo y Control

Área de conocimiento	Descripción	Grupo de procesos con los que se entrelaza
Gestión de la Calidad del proyecto	Asegurar que se satisfacen todos los requisitos	Planeación Ejecución Monitoreo y Control
Gestión de los Recursos del proyecto	Garantizar el uso efectivo de recursos, humanos y materiales.	Planeación Ejecución Monitoreo y Control
Gestión de las Comunicaciones del proyecto	Asegurar que la información sea oportuna y apropiada.	Planeación Ejecución Monitoreo y Control
Gestión de los Riesgos del proyecto	Minimizar el impacto de las posibles ocurrencias.	Planeación Ejecución Monitoreo y Control
Gestión de las Adquisiciones del proyecto	Adquirir los recursos necesarios por fuera del proyecto.	Planeación Ejecución Monitoreo y Control
Gestión de los Interesados del proyecto	Identificar personas o grupos de personas que pueden impactar o ser impactados por el proyecto, y desarrolla estrategias de relacionamiento con estos	Inicio Planeación Ejecución Monitoreo y Control

Fuente: Información obtenida y adaptado de Muñoz, I.L. Preparación Efectiva para el Examen PMP-CAMP , 2018

Tabla 2. Descripción de los grupos de procesos

Grupos de Procesos	Descripción general del foco de los procesos
Inicio	Autorización Formal del inicio de un Proyecto o fase
Planificación	Se desarrolla el plan para la dirección del proyecto
Ejecución	Ejecutar y completar el trabajo. Generar los Entregables
Monitoreo y Control	Observar e identificar los posibles problemas. Adoptar acciones correctivas.
Cierre	Finalización formal de todas las actividades del proyecto. Aceptación Formal del Proyecto

Fuente: Información obtenida y adaptado de Muñoz, I.L. Preparación Efectiva para el Examen PMP-CAMP ,2018

Los procesos contenidos en cada grupo pueden ser efectuados una vez, varias veces de forma periódica o constantemente a lo largo del proyecto, y están constituidos por unas entradas, herramientas, técnicas y Salidas, que, al relacionarse entre sí, crean una red en la que las salidas de un proceso pueden ser la entrada para iniciar otro. (Muñoz, 2018)

Actualmente, los riesgos sobre la seguridad de la información se identifican, y gestionan usando el área de conocimiento sobre la Gestión de Riesgos de los proyectos, la cual incluye los siguientes procesos (Project Management Institute, 2017):

- Grupo de Procesos de Planificación:

- Planificar la gestión de los riesgos
- Identificar los Riesgos
- Realizar el análisis Cualitativo de los riesgos
- Realizar el análisis cuantitativo de los riesgos
- Planificar la respuesta de los riesgos

- Grupo de procesos de Ejecución:
  - Implementar la respuesta a los riesgos
- Grupo de procesos de Monitoreo y Control:
  - Monitorear los Riesgos

3.1.2 Seguridad de la Información ISO/IEC 27001, Anexo A ISO 27002

Esta norma se desarrolla con el fin de que las organizaciones la puedan usar como referencia o documento guía para seleccionar e implementar controles aplicables a la seguridad de la información, teniendo en cuenta el entorno específico en el que se desarrollan (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013).

Establece que la seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, políticas, procesos, procedimientos, estructuras organizacionales y las funciones del software y del hardware (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013)

De esta forma, una política de la seguridad de la información debería contener declaraciones concernientes a (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013):

a) la definición de seguridad de la información, objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información;

b) la asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos;

c) procesos para manejar las desviaciones y las excepciones.

Dichas políticas deben tener implementados controles de seguridad de la información y estar estructuradas para tener en cuenta los temas de interés. Algunos ejemplos de las políticas mencionadas en la norma que podrían ser aplicables a proyectos son (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013):

- Controles de acceso
- Clasificación y manejo de la información
- Transferencia de información
- Dispositivos móviles
- Copias de respaldo
- Protección contra códigos Maliciosos
- Gestión de vulnerabilidades técnicas

- Seguridad de las comunicaciones
- Privacidad y protección de los datos personales.
- Relaciones con los proveedores.

De igual forma, la asignación de roles y responsabilidades para la seguridad de la información es una característica importante dentro de la norma, ya que esta especifica que se deben identificar, definir y documentar todas las responsabilidades para las actividades de seguridad de la información y gestión del riesgo, particularmente para la aceptación de riesgos residuales (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013).

Con relación a la seguridad de la información en los proyectos, la norma tiene un numeral corto y conciso, en el cual indica que “La seguridad de la información se debería tratar en la gestión de proyectos independientemente del tipo de proyectos” (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013).

Esta se debe integrar a los métodos de gestión de proyectos de la organización, y es aplicable a cualquier proyecto, independiente de la naturaleza del mismo.

La norma en el control 6.1.5 Seguridad de la información en la gestión de proyectos, establece que los métodos de gestión de proyectos que se usen deben requerir que (ISO/IEC 27002, 2013):

a) los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto

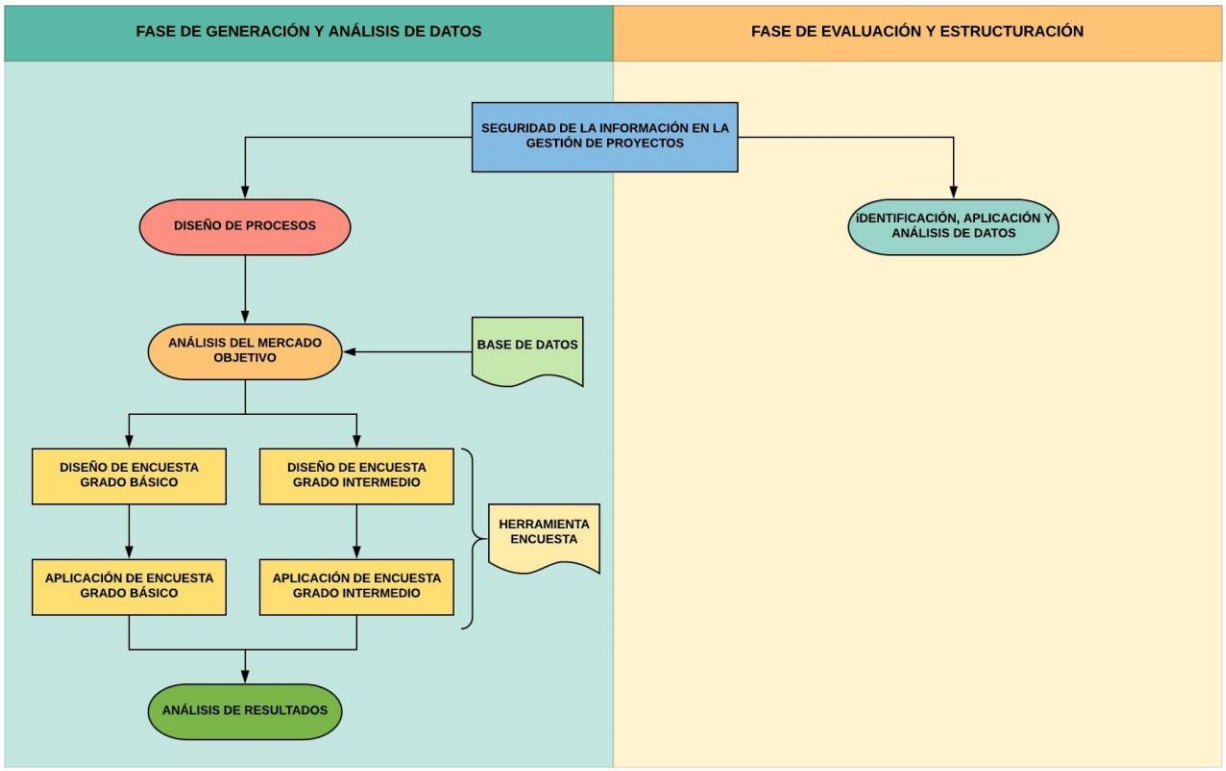
b) la valoración de los riesgos de seguridad de la información se lleva a cabo en una etapa temprana del proyecto, para identificar los controles necesarios.
c) La seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

Indica la importancia de revisar de forma regular las implicaciones de seguridad en todos los proyectos. Finalmente, hace hincapié en la importancia de la asignación responsabilidades al recomendar su definición e inclusión dentro de roles definidos en los métodos existentes de la gestión de proyectos. (ISO/IEC 27002, 2013) (ISO/IEC 27001 Anexo A, 2013)

4. Metodología

Para la elaboración de los nuevos planteamientos desarrollados en este trabajo se ejecutaron dos fases (ver ilustración 1.): La fase de generación y análisis de datos, donde se identificó el nicho de empresas como mercado objetivo para realizar un estudio exploratorio que se explica en cada una de las seis etapas que lo componen, y la fase de evaluación y estructuración cuyos resultados son derivados de las necesidades expuestas en la primera fase como requerimientos para la implementación de nuevas actividades que involucren la seguridad de la información en la dirección de proyectos.

Figura 1. Diagrama de Metodología



4.1 Fase de generación y análisis de datos

4.1.1 Análisis de mercado objetivo

Según la Guía para la Implementación de Seguridad de la Información en una MIPYME en su versión 1.2 del 6 de Noviembre de 2016 menciona: “Las MIPYMES suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridades olvidadas” (MINTIC, 2016) es decir, que son este tipo de empresas las que tiene menor probabilidad de incluir dentro de sus procesos de gestión de proyectos, políticas y procedimientos que mitiguen el riesgo en la disponibilidad, confidencialidad e integridad de la información convirtiéndose en el objetivo de estudio en esta fase de investigación. Añadiendo la restricción del sector económico en informática y comunicaciones catalogado con uno de los de mayor crecimiento en Colombia durante los últimos años.

Se revisó la Clasificación Industrial Internacional Uniforme de todas las actividades económicas (CIIU) publicada por el DANE, entidad que organiza las empresas según su actividad principal, catalogando en los niveles de sección, división, grupo y clase.

Como primer nivel se adoptó la sección J (Información y comunicaciones). Esta sección incluye la producción y la distribución de información y productos culturales, el suministro de los medios para transmitir o distribuir esos productos, así como de datos o de comunicaciones,

actividades de tecnologías de información y el procesamiento de datos y otras actividades de servicios de información.

Teniendo en cuenta las empresas que podrían ejecutar proyectos, siguiendo algún marco teórico de buenas prácticas, se incluyeron las siguientes divisiones:

División 58. Actividades de edición

División 61. Telecomunicaciones

División 62. Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas.

División 63. Actividades de servicios de información.

Seleccionando de esta división las clases resaltadas en la Tabla 3.

Tabla 3. Clases de actividades económicas seleccionadas**.**

División	Grupo	Clase	Descripción
58	-	-	Actividades de Edición
-	-	5820	Edición de programas de informática (software)
61	-	-	Telecomunicaciones
-	611	6110	Actividades de telecomunicaciones alámbricas
-	612	6120	Actividades de telecomunicaciones inalámbricas
-	613	6130	Actividades de Telecomunicaciones Satelitales
-	619	6190	Otras Actividades de Telecomunicaciones
62	-	-	Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Consultoría informática y actividades relacionadas
-	620	-	Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Consultoría informática y actividades relacionadas

División	Grupo	Clase	Descripción
-	-	6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas).
-	-	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas.
-	-	6209	Otras actividades de tecnologías de información y actividades de servicios informáticos.
63	-	-	Actividades de servicios de información
-	631	-	Procesamiento de datos, alojamiento y actividades relacionadas; portales web
-	-	6311	Procesamiento de datos, alojamiento (hosting) y actividades relacionadas
-	-	6312	Portales web
-	639	-	Otras actividades de servicio de información
-	-	6391	Actividades de agencia de noticias
-	-	6399	Otras actividades de servicio de información n.c.p.

Fuente: Tomado de Clasificación Industrial Internacional Uniforme De Todas Las actividades Económicas, revisión 4 Para Colombia. (DANE)

Según base de datos adquirida en la cámara y comercio de Cali, para el 2018, existen 1081 empresas bajo la categoría de persona jurídica según las características mencionadas, de las cuales 18 son Medianas empresas, 163 Pequeñas empresas y 900 Microempresas, distribuidas por actividad económica de la siguiente forma: (Ver Tabla 4. Cantidad de MiPymes según las actividades económicas seleccionadas)

Tabla 4. Cantidad de MiPymes existentes según las actividades económicas seleccionadas

COD_CIUU	DESCRIPCION_CIUU	Med	Peq	Mic	Total, general
5820	EDICIÓN DE PROGRAMAS DE INFORMÁTICA (SOFTWARE)		4	30	34
6110	ACTIVIDADES DE TELECOMUNICACIONES ALÁMBRICAS		6	34	40
6120	ACTIVIDADES DE TELECOMUNICACIONES INALÁMBRICAS	2	5	40	47
6130	ACTIVIDADES DE TELECOMUNICACIÓN SATELITAL			6	6
6190	OTRAS ACTIVIDADES DE TELECOMUNICACIONES	2	20	108	130

COD_CIUU	DESCRIPCION_CIUU	Med	Peq	Mic	Total, general
6201	ACTIVIDADES DE DESARROLLO DE SISTEMAS INFORMÁTICOS (PLANIFICACIÓN, ANÁLISIS, DISEÑO, PROGRAMACIÓN, PRUEBAS)	5	50	313	368
6202	ACTIVIDADES DE CONSULTORÍA INFORMÁTICA Y ACTIVIDADES DE ADMINISTRACIÓN DE INSTALACIONES INFORMÁTICAS	6	49	194	249
6209	OTRAS ACTIVIDADES DE TECNOLOGÍAS DE INFORMACIÓN Y ACTIVIDADES DE SERVICIOS INFORMÁTICOS		14	82	96
6311	PROCESAMIENTO DE DATOS, ALOJAMIENTO	1	9	44	54

COD_CIUU	DESCRIPCION_CIUU	Med	Peq	Mic	Total, general
	HOSTING) Y ACTIVIDADES RELACIONADAS				
6312	PORTALES WEB			31	31
6391	ACTIVIDADES DE AGENCIAS DE NOTICIAS			3	3
6399	OTRAS ACTIVIDADES DE SERVICIO DE INFORMACIÓN N.C.P.	2	6	15	23
	TOTAL	18	163	900	1081

Fuente: Tomado de Clasificación Industrial Internacional Uniforme De Todas Las actividades Económicas, revisión 4 Para Colombia. (DANE)

Teniendo en cuenta la cantidad de empresas que arroja la muestra y que a la fecha no se cuenta con estudios previos en las MiPymes sobre las buenas prácticas en la gestión de proyectos y seguridad de la información, se realiza una investigación exploratoria, ofreciendo un primer acercamiento al problema que permita identificar y proponer las actividades que apoyen la disponibilidad, confidencialidad e integridad de la información durante la ejecución de uno o varios de los cinco grupos de procesos enmarcados por el PMBOK® para la buena gestión de proyectos.

Según Ildefonso Grande Esteban y Elena Abascal Fernández en el libro Fundamentos y Técnicas de Investigación Comercial 12ª Edición 2014, las investigaciones exploratorias pueden tener por objeto conocer situaciones, problemas o fenómenos con mayor profundidad, identificando posibles cursos de acción (Esteban & Fernández, 2014).

A partir del tipo de investigación exploratoria, de las 1081 empresas se obtiene una muestra representativa de 99 empresas de aquellas que ejecuta una o varias de las actividades económicas seleccionadas, calculada mediante el uso de la fórmula para cálculo de muestra de poblaciones finitas con un nivel de confiabilidad del 94% y un margen de error del 9%:

$$n = \frac{N \times Z_{\alpha}^{2} \times p \times q}{d^{2} \times (N-1) + Z_{\alpha}^{2} \times p \times q}$$

Donde:

N = Tamaño Total de la población

Z_{α} = Nivel de confianza

P = Probabilidad del éxito o proporción esperada

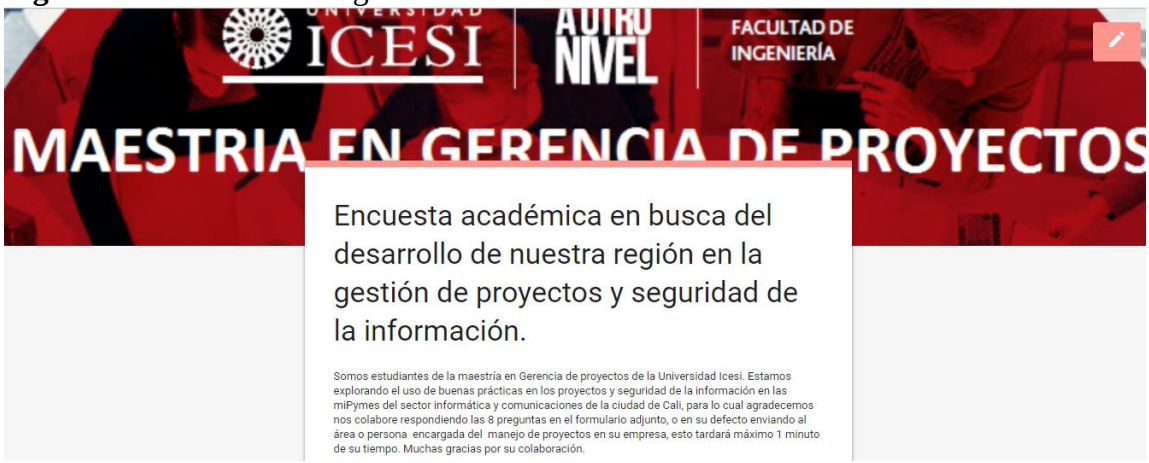
q = Probabilidad de fracaso

d = Precisión (error máximo admisible)

La elección de las empresas participantes se realizó al azar mediante la creación de un aleatorio en el programa estadístico Excel.

Diseño de encuesta grado básico: Para el nivel básico exploratorio sobre el uso de las buenas prácticas en la ejecución de proyectos y seguridad de la información, se utiliza el medio digital como captura, bajo la herramienta de formularios en Google, donde se diseñan 8 preguntas dividas en dos secciones, 4 focalizadas en la gerencia de proyectos y 4 en la seguridad de la información, y el objetivo principal es conocer qué tipo de metodología y herramientas utilizan las MiPymes para estos sistemas de gestión y control, además si las empresas cuentan con personas capacitadas en los temas.

Figura 2. Portada encuesta grado básico



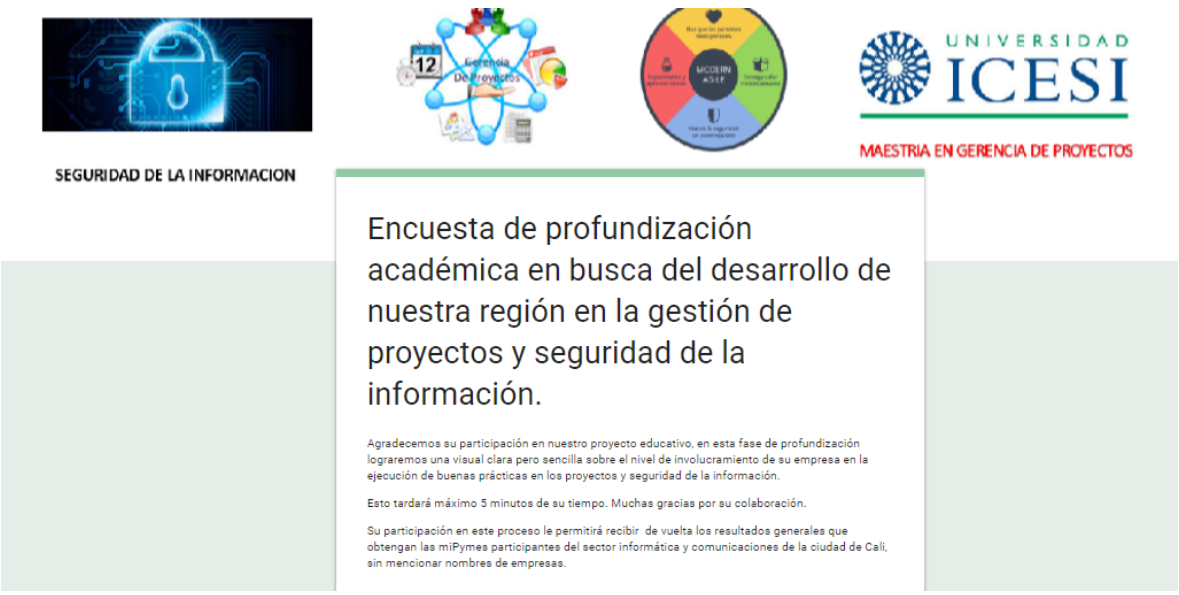
Aplicación encuesta grado básico:

Se envían las encuestas a las 99 empresas seleccionadas anteriormente, a los correos de las personas con roles de alta gerencia o gerencia media dentro de la organización.

Diseño de encuesta grado intermedio: En el nivel exploratorio intermedio con una intención de obtener mayor profundidad en la información, se diseña, con la herramienta de formularios en Google, 23 preguntas con requerimientos más específicos de información, 10 preguntas cerradas

sobre el manejo de metodología, políticas, roles y planes que apoyen la disponibilidad, confidencialidad e integridad de la información, y 13 preguntas de clasificación donde podemos medir el tipo de metodología y técnicas para buena gestión de proyectos según el marco utilizado por cada organización.

Figura 3. Portada encuesta grado intermedio



Aplicación encuesta grado intermedio: Se envía la encuesta de profundización a las empresas que participan en la fase inicial de grado básico.

Análisis de resultados: Con ayuda de las encuestas se planea conocer si las empresas que trabajan con proyectos tienen conocimiento sobre buenas prácticas en su administración, y si reconocen la importancia de garantizar la disponibilidad, confidencialidad e integridad de la información manejada dentro de dichos proyectos, además de determinar en qué medida tienen conocimiento de la normativa en relación con la gestión de la seguridad de la información, los

marcos relacionados a la misma y las razones por las cuales aún no se considera la implementación de buenas prácticas de gestión de seguridad de la información durante la dirección de los proyectos.

En la segunda encuesta, se busca profundizar sobre las metodologías usadas en la dirección de proyectos y el manejo de la seguridad de la información.

4.1.2 Identificación, aplicación y análisis de datos

La segunda fase de evaluación y estructuración es una única etapa con el diseño de la propuesta que nos ayuda a incluir nuevos procesos en la dirección de proyectos con el fin de apoyar la disponibilidad, confidencialidad e integridad de la información. Usando como base los lineamientos de entradas, herramientas y salidas establecidos dentro de los cinco grupos de procesos (inicio, planeación, ejecución, monitoreo y control y cierre) especificados en la guía de fundamentos para la dirección de Proyectos (Guía PMBOK®), enlazado con los requerimientos que sugiere la norma internacional ISO/IEC 27001 Anexo A e ISO/IEC 27002, como directriz de gestión de la seguridad de la información, específicamente en el numeral 6.1.5 seguridad de la información en la gestión de proyectos.

5. Resultados obtenidos

5.1 Resultado obtenidos encuesta grado básico

Como resultado de la aplicación de la primera encuesta, se obtiene una descripción general sobre las percepciones de las empresas frente al desarrollo de proyectos, la aplicación de sistemas de seguridad de la información y la necesidad de contar con buenas prácticas de dirección de proyectos y seguridad de la información como medio para dar cumplimiento a sus requerimientos y garantizar una alta rentabilidad.

A pesar de que se abordó al 100% de la población seleccionada, hubo una baja disposición de respuesta por parte de los encuestados, por lo cual se obtuvo un solo un total de 74 respuestas de las cuales más del 75% fueron de microempresas como se muestra en la siguiente tabla:

Tabla 5. Cantidad de empresas encuestadas

Tipo de empresa	Cantidad
Microempresa	56
Pequeña	15
Mediana	3
Total	74

En cuanto a su actividad económica, hubo una mayor participación de las empresas que desarrollan sistemas informáticos, seguido por las organizaciones que realizan consultoría en informática y actividades de administración de instalaciones informáticas.

Del total de 74 empresas, 71 declararon desarrollar proyectos para los clientes, donde más del 80%, tienen roles capacitados en administración de proyectos y usan un marco metodológico siendo los más usados PMBOK® para proyectos predictivos y SCRUM para Agiles, muchas veces aplicados de forma hibrida, mezclando herramientas adoptadas de cada uno según los requerimientos de cada proyecto. A su vez, el 59% de las organizaciones con proyectos, cuenta además con una herramienta tecnológica para soportar los proyectos de los clientes, dentro de las más usadas están Microsoft Project, Jira, y 5 empresas dijeron usar Desarrollos internos de la compañía. De esto se comprende que las empresas participantes conocen y manejan los aspectos base de la dirección de proyectos, los roles, marcos de trabajo y herramientas.

En relación a la gestión de seguridad de la información, 70 empresas reconocieron que los clientes requieren que se les garantice la disponibilidad, confidencialidad e integridad de la información de los proyectos que dirigen, sin embargo, un poco menos del 50% de estas empresas usan un marco metodológico para la seguridad de la información y sus riesgos, siendo la Norma ISO 27001 la más reconocida, seguida de la ISO 27002 e ISO 31000.

En contraste con los resultados obtenidos para la administración de proyectos, se puede apreciar que si bien en las organizaciones que contestaron la encuesta hay un reconocimiento relativamente alto de la necesidad del manejo de la seguridad de la información dentro de los

proyectos, menos de la mitad tiene nociones sobre la existencia de una normativa y marcos de trabajo que permiten aplicarla de manera efectiva. Lo cual lleva a reforzar la afirmación de que las MiPymes son empresas con poca probabilidad de gestionar la seguridad de la información durante el desarrollo de sus proyectos.

Finalmente, cuando se les pregunta sobre cuál consideran es el principal obstáculo para no contar con buenas prácticas de proyectos y sistemas de gestión de seguridad de la información que le permitan obtener mejores resultados, las razones más frecuentes fueron el costo de la inversión, el tiempo que debe ser dedicado a la implementación y la falta de recursos humanos con capacitación en el área. Adicionalmente, hubo 10 empresas que declararon que para ellos no era necesario implementar un marco o herramientas, ya que podrían trabajar con lo que tuviera el cliente.

5.2 Resultado obtenidos encuesta grado intermedio.

Con el objetivo de ofrecer mayor profundidad en la información sobre el manejo de proyectos y seguridad de la información, se envió la encuesta de profundización a las 74 empresas, de las cuales se había obtenido respuesta en la fase inicial de grado básico, sin embargo, en esta ocasión el nivel de resistencia fue mayor y hubo menos respuestas, incluso siendo necesario acudir a otros medios digitales y telefónicos, finalmente, se logran 19 respuestas en esta fase del proyecto.

Participaron 2 empresas medianas, 3 pequeñas y 14 microempresas, con mayor participación de las empresas cuya actividad económica es el Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) con el 42% (8), seguida por 26% (5) correspondiente a empresas de consultoría informática y actividades de administración de instalaciones informáticas.

Gestión de los Riesgos.

Con respecto al manejo de técnicas de gestión del riesgo 16 de las 19 empresas encuestadas, reportan usarlas algunas veces para medir y evaluar el impacto del riesgo durante la ejecución de los proyectos, no obstante, 12 de las 16, dice no contar en su organización con alguna metodología de riesgo estandarizada, sin embargo, la mayor preocupación para la gerencia debe estar representado en que el 47% (9) de estas empresas no tienen identificados los riesgos de seguridad de la información a los cuales están expuestos los activos de información.

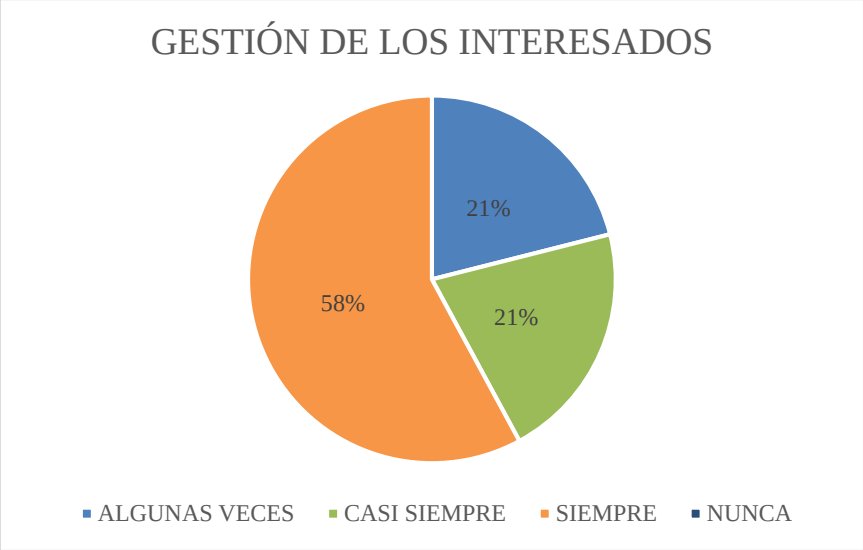
Activos de información.

El 58% (11) cuenta con un inventario actualizado y clasificado de acuerdo con la criticidad de los activos de información de la organización, sin embargo, solo el 45% (5) de estas, tiene identificado los riesgos a los cuales están expuestos sus activos de la información.

Gestión de interesados.

El identificar a las personas, grupos y organizaciones involucradas en el proyecto desde la etapa de inicio, es un proceso con mayor aceptación en las empresas, considerando su alto nivel de importancia.

Grafico 1.Empresas encuestadas que realizan el proceso de identificación y gestión de los interesados del proyecto



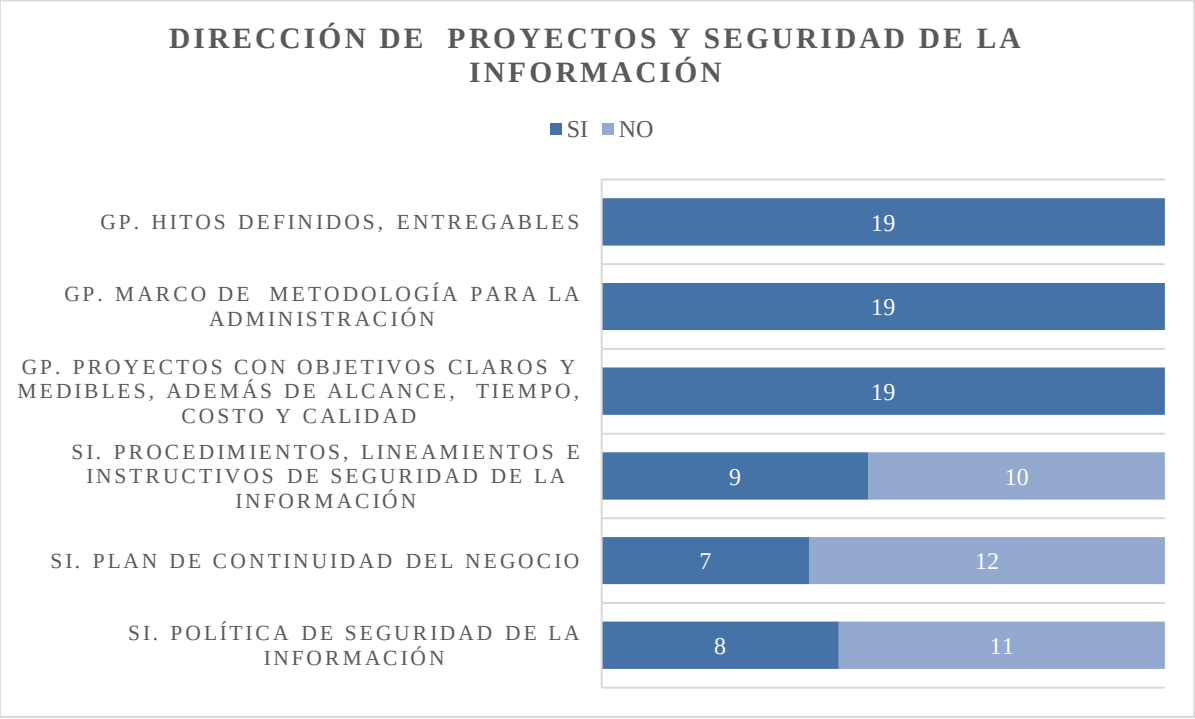
Sin embargo, al manejar interesados en el proyecto, también se hace relevante contar con esquemas de clasificación de la información, como público, semiprivado, privado y sensible, pero, en este proceso solo el 42% (8) de las MiPymes encuestadas son conscientes de estos requerimientos.

Gerencia de proyectos y Seguridad de la información.

Comparando las respuestas obtenidas entre el área de gerencia de proyectos y el de la seguridad de la información, se observa mayor inclinación de las empresas en manejar metodologías y procesos para la gestión de proyectos. Un promedio del 57% de la MiPymes no ejecutan políticas ni procedimientos que apoyen la seguridad de la información dentro de la

organización, en cambio, el 100% realiza proyectos con lineamientos específicos de algún marco metodológico.

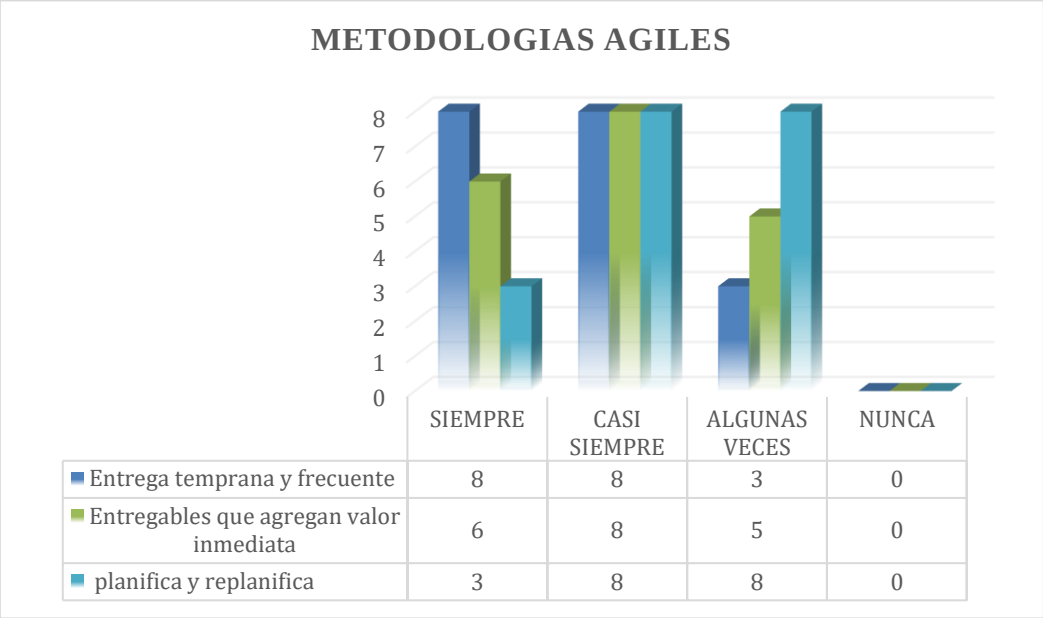
Grafico 2.Aplicación de buenas prácticas en la dirección de proyectos y en la seguridad de la información



De forma similar a los resultados de la primera encuesta, en esta fase también se identifica mayor desarrollo de gestión en buenas prácticas de proyectos que en Seguridad de la información y, aunque las empresas del sector encuestado reconocen la importancia de garantizar la integridad, confidencialidad y disponibilidad de la información, un poco más del 50% no siguen los lineamientos que promueven los marcos metodológicos para la seguridad de la información. Evidenciando la seguridad información con el área más vulnerable durante la gestión efectiva de proyectos.

Metodologías Ágiles.

Grafico 3. Respuesta de las organizaciones participantes al uso de metodologías Agiles



	SIEMPRE	CASI SIEMPRE	ALGUNAS VECES	NUNCA
Entrega temprana y frecuente	8	8	3	0
Entregables que agregan valor inmediata	6	8	5	0
planifica y replanifica	3	8	8	0

En las empresas encuestadas, se evidencia una inclinación por metodologías que incitan a la entrega de productos mínimos viables, ya que todas aseguran ofrecer en algún momento, trabajos con entregas de valor temprano y ciclos de retroalimentación.

Sin embargo, la mayoría de los participantes (12) prefiere abordar trabajos de alta incertidumbre sólo algunas veces. Esto evidencia que las organizaciones participantes no tienen un nivel alto de tolerancia al riesgo, por lo cual es mucho más importante que se fortalezcan las medidas de gestión de riesgos.

Roles y responsabilidades.

El 63% (12) de las empresas cuentan con personas dentro de su organización capacitados en administración de proyectos, para garantizar el uso de las buenas prácticas, sin embargo, solo el 42% (5) de estas 12 empresas, tienen un esquema de roles y responsabilidades definidos dentro de la organización para la seguridad de la información. Esto evidencia una vez más que las buenas prácticas en dirección de proyectos son en cierta medida aplicadas y aceptadas dentro de las organizaciones, pero aún no hay un reconocimiento de los marcos de trabajo para la seguridad de la información o la necesidad de implementarlos.

6. Presentación de la propuesta

6.1 Propuesta de procesos para la gestión de la seguridad de la información dentro de la dirección de proyectos. Marco PMBOK®

Las metodologías alrededor de la dirección de proyectos enmarcan como propuesta de valor el uso buenas prácticas en las diferentes fases del proyecto. Sin embargo, se ha identificado por medio de encuestas a las Medianas, Pequeñas y Microempresas del sector de Tecnología de información y comunicaciones en la ciudad de Cali, la necesidad de incluir en su campo de acción la seguridad de la información mediante la implementación de políticas, procedimientos y controles que garanticen un sistema de gestión acorde al tipo de empresa y proyecto, de forma que se puedan desarrollar acciones que aumenten la probabilidad de éxito en los proyectos.

La seguridad de la información debe ser tratada durante la dirección de todo tipo de proyectos, integrando la disponibilidad, confidencialidad e integridad de la información en las metodologías y procesos para gestión del mismo. De esta forma, la identificación y monitoreo de los riesgos en seguridad de la información deben ser parte del proyecto (ISO/IEC 27002, 2013).

Uno de los objetivos mencionados por la ISO 27002 numeral 6.1.5, para la Seguridad de la información en la gestión de proyectos requiere incluir la seguridad de la información como parte de todas las fases de la metodología del proyecto. Es por esto que nuestra propuesta se basa en la inclusión de un área de conocimiento en el marco metodológico para la dirección de proyectos PMBOK®, incluyendo procesos para resguardar y proteger la información desde el

inicio hasta la culminación del mismo. Basados en la estructura propuesta por el marco metodológico PMBOK® a continuación se muestra la Gestión de la Seguridad de la información como área de conocimiento para la gestión de proyectos (Tabla 6 presentación del área de gestión de seguridad de la información del proyecto).

Tabla 6. Presentación del área de gestión de seguridad de la información del proyecto.

	Grupo de Procesos de la Dirección de Proyectos				
Áreas de Conocimiento	Grupo de procesos de Inicio	Grupo de procesos de Planeación	Grupo de procesos de Ejecución	Grupo de procesos de Monitoreo y control	Grupo de procesos de Cierre
Gestión de la Integración del Proyecto	-	-	-	-	-
Gestión del Alcance		-		-	
Gestión del Cronograma del Proyecto		-		-	
Gestión del Costo del Proyecto		-		-	
Gestión de la Calidad del Proyecto		-	-	-	
Gestión de los Recursos del Proyecto		-	-	-	
Gestión de las Comunicaciones del Proyecto		-	-	-	
Gestión de los Riesgos del Proyecto		-	-	-	

Áreas de Conocimiento	Grupo de Procesos de la Dirección de Proyectos				
	Grupo de procesos de Inicio	Grupo de procesos de Planeación	Grupo de procesos de Ejecución	Grupo de procesos de Monitoreo y control	Grupo de procesos de Cierre
Gestión de las Adquisiciones del Proyecto		-	-	-	
Gestión de los Interesados del Proyecto	-	-	-	-	
Gestión de la Seguridad de la información del Proyecto	Desarrollar el acta de constitución frente a la seguridad de la información.	Identificar y Valorar los riesgos de seguridad de la información. Planificar los controles de Seguridad de la Información.	Implementar los controles de Seguridad de la Información.	Monitorear los controles de Seguridad de la Información.	Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información.

Fuente: Cuadro Adaptado del PMBOK®. (Project Management Institute, 2017)

ÁREA DEL CONOCIMIENTO: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Esta área de conocimiento centra su valor en las políticas, procesos, procedimientos, controles, estructuras organizacionales y funciones de software y hardware que garanticen la disponibilidad, confidencialidad e integridad de la información durante la gestión del proyecto. Al igual que el área de integración desarrollada por el PMBOK®, la gestión de seguridad de la información cuenta con procesos en cada uno de los 5 grupos de procesos, inicio, planificación, ejecución, monitoreo y control y cierre. Con el fin de proteger los activos del proyecto durante todas etapas.

Grupo de procesos a los cuales pertenecen cada proceso de la Gestión de Seguridad de la Información (Ver tabla 7).

Tabla 7.Grupos de procesos a los cuales pertenecen los procesos de la gestión de la seguridad de la información

GRUPO DE PROCESOS	PROCESOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Inicio	Desarrollar el acta de constitución frente a la Seguridad de la Información
Planificación	Identificar y valorar los riesgos de la seguridad de la Información Planificar los controles de seguridad de la Información
Ejecución	Implementar los controles de seguridad de la información
Monitoreo y Control	Monitorear los Controles de seguridad de la Información
Cierre	Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información

En el área de conocimiento de gestión de la seguridad de la información, es importante conocer las principales salidas que son derivadas de cada proceso. Es por esto, que se hace un resumen de las principales salidas en el cuadro a continuación (ver tabla 8):

Tabla 8. Principales salidas de los procesos de la gestión de la seguridad de la información

PROCESOS	SALIDAS CLAVE
Desarrollar el acta de constitución frente a la Seguridad de la Información	Acta de seguridad de la información Acuerdo de Confidencialidad para el proyecto
Identificar y valorar los riesgos de seguridad de la Información	Registro de riesgos de seguridad de la información
Planificar los controles de seguridad de la Información	Política de seguridad de la información para la dirección del proyecto Controles de seguridad de la información

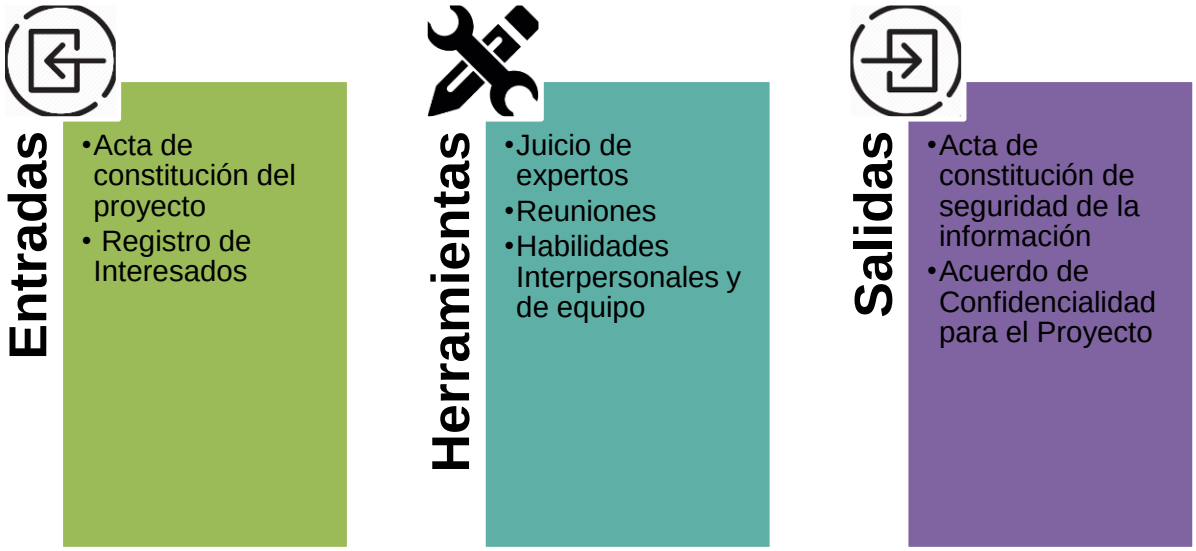
PROCESOS	SALIDAS CLAVE
	Inventario de los activos de información
Implementar los controles de seguridad de la información	Registro de incidentes de la seguridad de la información Datos de desempeño en seguridad de la Información Solicitudes de Cambio Actualizaciones a la política de seguridad de la información
Monitorear los Controles de seguridad de la Información	Informes de desempeño en seguridad de la información Solicitudes de Cambio Actualizaciones a la política de seguridad de la información Registro de Incidentes de la Seguridad de la Información
Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información	Informe Final Inventario actualizado de los activos de información

PROCESO: Desarrollar el acta de constitución frente a la seguridad de la información

En este proceso se desarrolla el acta de constitución frente a la seguridad de la información, donde se describen y presentan formalmente el alcance, los límites y lineamientos generales que tendrá la gestión de la seguridad de la información durante el proyecto. Aquí el patrocinador da su aprobación y las partes se comprometen a asegurar la seguridad de la información durante el proyecto.

A continuación, se presentan las entradas, herramientas y salidas de este proceso.

Figura 4.Entradas, Herramientas y Salidas para el Proceso Desarrollar el acta de constitución frente a la seguridad de la información



Entradas:

Acta de Constitución del Proyecto: Documento que formaliza y da el punto de partida al proyecto. En éste se da la autorización y guía para el desarrollo del plan para la dirección del proyecto, se describe el trabajo a realizar, los supuestos, restricciones y riesgos generales del proyecto.

Registro de Interesados: Contiene información sobre la ubicación de los interesados en proyecto, el puesto en la organización, el rol en el proyecto, la fase del ciclo de vida donde el interesado va a tener más influencia en el proyecto, qué nivel puede tener un interesado de poder, interés, influencia, etc.

Herramientas:

Juicio de Expertos: El juicio de expertos proporciona la opción de obtener una opinión u orientación de cualquier persona experta, ya sea interna o externa, con conocimientos tanto técnicos como legales, en relación con la seguridad de la información, su regulación y redacción de acuerdos de confidencialidad.

Reuniones: espacios donde es importante identificar junto con los interesados clave, los riesgos generales que puedan existir con respecto a la seguridad de la información, criterios para determinar los puntos de control, la clasificación de la información que se va a manejar a lo largo del proyecto, las responsabilidades sobre la misma, y otros aspectos a definir para el acuerdo.

Habilidades interpersonales y de Equipo: En este proceso se necesitan habilidades como la gestión de conflictos, para alinear a los interesados; facilitación para garantizar la participación de todos los interesados y la toma de decisiones; Gestión de reuniones, se necesita tener una buena gestión de reuniones dada la frecuencia de estas.

Salidas:

Acta de Constitución de seguridad de la Información: En este documento se da el primer acercamiento en el cual se presentan formalmente el alcance y los límites que se le dará a la gestión de la seguridad de la información con relación a las características del proyecto, la organización, y otros factores como la tecnología y activos de la información. Se da la aprobación por parte del patrocinador. Un aspecto importante de este documento es que relaciona los objetivos de la seguridad de la información con los objetivos del proyecto.

En general este documento puede tener:

- Objetivos generales
- Marco de referencia regulatorio
- Requisitos del proyecto frente a la seguridad de la información
- Principales riesgos relacionados a la seguridad de la información
- Principales supuestos
- Clasificación de la información que se manejará en el proyecto
- Niveles de acceso a la información del proyecto
- Quién tendrá dichos accesos
- Puntos generales de control
- Funciones y Responsabilidades de los interesados

En este documento se presentan los requisitos sobre la seguridad de la información que deben cumplirse durante el proyecto, riesgos, interesados y responsabilidades y accesos clave.

Acuerdo de Confidencialidad del Proyecto: Acuerdo legal que se hace entre el patrocinador, el cliente y el director del proyecto, donde se establecen las condiciones bajo las cuales se tratará la información involucrada en el proyecto, de modo que se restrinja su uso y se salvaguarde la confidencialidad e integridad de esta.

PROCESO: Identificar y valorar los riesgos de seguridad de la información

En este proceso se determinan y documentan los riesgos individuales sobre la seguridad de la información, se describen las causas, responsables y posibles respuestas. Se saca una lista de amenazas y oportunidades que pueden impactar a los activos de la información, la comunicación y la confidencialidad, disponibilidad e integridad de datos.

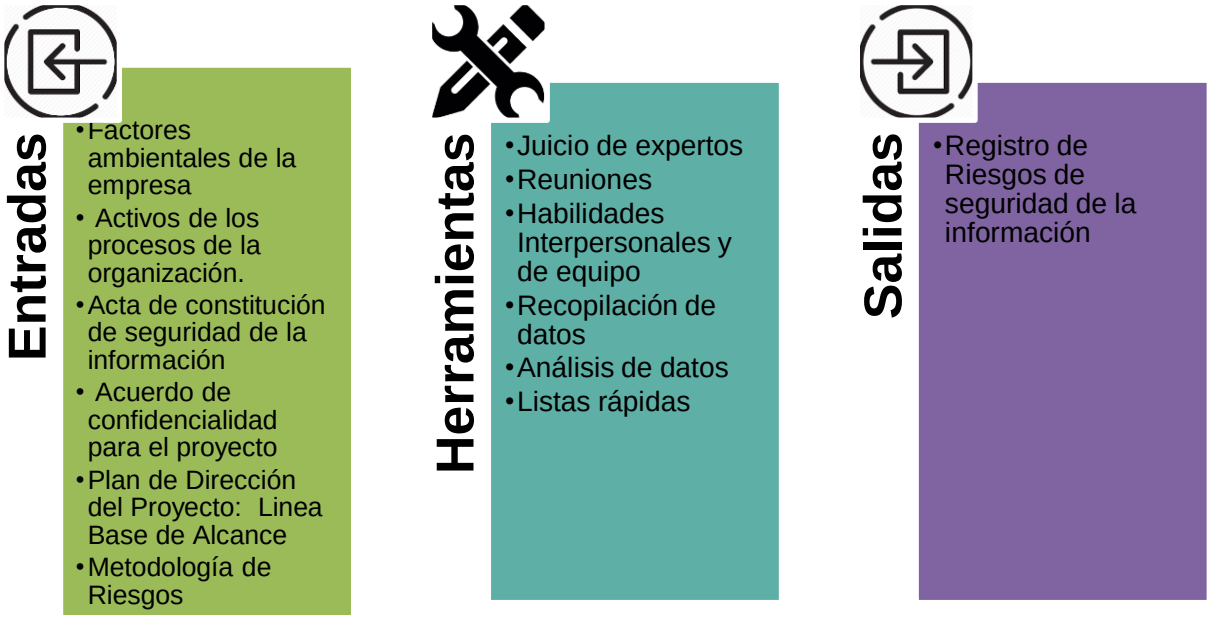
También se incluye una valoración cualitativa de los riesgos identificados, evaluando y combinando la probabilidad de ocurrencia y el impacto de dichos riesgos.

En este documento se incluye la identificación de los puntos críticos de control que se deben ser marcados en el ciclo de vida del proyecto, teniendo en cuenta que en éstos es donde se deben implementar controles preventivos y de seguridad.

Este proceso es iterativo, ya que los riesgos sobre la seguridad de la información y los posibles puntos de control pueden ser identificados a medida que se desarrolla el proyecto y es necesario actualizar las listas.

A continuación, se describen las entradas, herramientas y salidas de este proceso:

Figura 5.Entradas, Herramientas y Salidas para el proceso Identificar y valorar los riesgos de seguridad de la información



Entradas:

Factores ambientales de la empresa: En este proceso se deben tener en cuenta factores internos como los procesos de la organización, su cultura, la infraestructura de redes y soporte, la administración del personal en temas de contratación, turnos, capacitación, sistemas de autorización de trabajos en la organización, entre otros. Al igual que factores externos como la normativa, guías y regulaciones que tengan dentro de su alcance el manejo de los sistemas de gestión de la seguridad de la información.

Activos de los procesos de la Organización: Se deben revisar todos los procesos operativos estándar, guías estandarizadas o instrucciones de trabajo que existan sobre la gestión de la información dentro de la organización. También se pueden tener en cuenta datos históricos,

lecciones aprendidas, bases de datos, niveles de autoridad, metodologías generales de análisis de peligros y puntos críticos de control.

Acta de Constitución de seguridad de la información: Este documento contiene la descripción general referente al alcance de la gestión de la seguridad de la información dentro del proyecto. Tiene la clasificación de la información, la descripción de los accesos, principales riesgos y supuestos además de tener ya un esquema base sobre los principales puntos de control identificados.

Acuerdo de confidencialidad para el proyecto: Este acuerdo contiene las condiciones bajo las cuales se tratará la información involucrada en el proyecto, de modo que se restrinja su uso y se salvaguarde la confidencialidad e integridad de la misma. Proporciona información importante sobre los riesgos identificados durante el proceso de preparación del acuerdo, al igual qué puntos críticos del proceso ya tienen un respaldo legal y cuáles estarían expuestos.

Plan de Dirección del Proyecto, Línea Base de Alcance: La línea base del alcance contiene la estructura de desglose del trabajo y su diccionario. Permite visualizar e identificar las actividades donde se presenta mayor incertidumbre con relación al manejo de la información, al igual de servir como marco para ubicar los puntos críticos de control dentro del desarrollo del proyecto.

Metodología de Riesgos: Esta entrada proporciona varias opciones para aplicar durante la valoración de los riesgos identificados. Pueden identificarse métodos que se implementen apoyados en juicios subjetivos o de forma más detallada por medio de cálculos de ocurrencia.

Herramientas:

Juicio de Expertos: En este proceso es altamente recomendable acudir a personas que tengan la experiencia y el conocimiento técnico necesario en el área para aportar en la identificación de riesgos de seguridad de la información y puntos críticos de control. Es un proceso complejo en el cual se requiere garantizar que se identifiquen el mayor número de riesgos para la seguridad de la información y puntos de control.

Reuniones: Se abren espacios con los interesados donde se discuten los posibles riesgos en la seguridad de la información con el fin de enriquecer la lista de riesgos identificados.

Habilidades Interpersonales y de equipo: En este proceso se necesitan habilidades facilitación para garantizar la participación de todos los interesados, establecer y seguir un método de trabajo y garantizar que toda la información del riesgo sea descrita de forma clara y completa.

Recopilación de datos: Se refiere al uso de técnicas y herramientas que pueden ser usadas en este proceso para recopilar los datos primarios. Entre las más comunes están la tormenta de ideas, las entrevistas, las encuestas, cuestionarios, métodos de observación, listas de verificación, diagramas de flujo, etc

Análisis de datos: Hay varias técnicas que pueden ser usadas con el objetivo de proporcionar validez, y apoyo a los datos antes recopilados. Ayuda a concluir y relacionar causas y resultados. Las técnicas generalmente usadas para estos casos son: Análisis de causa raíz, análisis DOFA, análisis de supuestos, análisis de la documentación.

Listas rápidas: Son un marco que puede ser usado para la generación de ideas, donde se usen técnicas para la identificación de los riesgos de la seguridad de la información o los puntos críticos de control.

Salidas:

Registro de Riesgos de seguridad de la información: La disposición y contenido de este documento varía dependiendo de las características de la organización frente a la gestión de los riesgos, sin embargo, por lo general en este documento se documentan de forma individual los riesgos de seguridad de la información que se han identificado, describiendo su causa raíz, responsables, respuestas y su respectiva valoración teniendo en cuenta la probabilidad y el impacto de cada uno. Es importante resaltar que este documento debe ser revisado y actualizado de forma constante durante la duración del proyecto.

En este documento también se describen las actividades que son críticas para el proyecto, donde hay alta vulnerabilidad y es necesario implementar un punto de control preventivo.

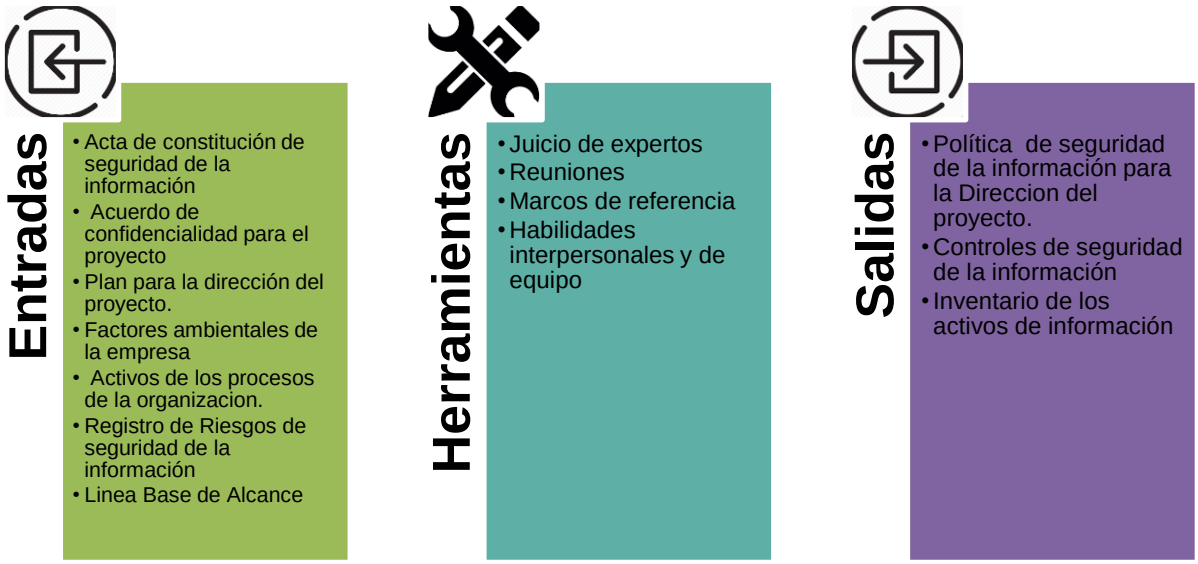
PROCESO: Planificar los controles de Seguridad de la Información.

En este proceso se desarrolla un documento o una serie de documentos relacionados donde se define la política de seguridad de la información que se usará para la dirección del proyecto. Aquí se definen los objetivos y principios por los cuales se orientan todas las actividades del proyecto que estén relacionadas a la seguridad de la información.

De esta forma, se emite de forma centralizada una directriz firmada por la alta dirección que debe ser conocida por todas las partes del proyecto y los interesados externos para los cuales se defina la necesidad.

A continuación, se presentan las entradas, herramientas y salidas de este proceso:

Figura 6.Entradas, Herramientas y Salidas para el proceso Planificar los controles de Seguridad de la Información



Entradas:

Acta de constitución de la seguridad de la Información: Aquí se encuentra descrita la información general que existe sobre la gestión de la seguridad de la información en el proyecto. Proporciona información sobre el alcance, las limitaciones, los supuestos, clasificación de la información, accesos y responsables.

Acuerdo de confidencialidad para el proyecto: Contiene las condiciones bajo las cuales las partes acordaron el tratamiento de la información del proyecto, las restricciones, responsabilidades legales, riesgos principales.

Plan para la dirección del Proyecto: El plan para la dirección del proyecto contiene todos los planes realizados en todas las áreas de conocimiento:

- Plan de gestión de requisitos
- Plan de gestión del cronograma
- Plan de gestión de los costos
- Plan de gestión de la calidad
- Plan de gestión de los recursos
- Línea base del alcance
- Línea base del cronograma
- Línea base de costos

En estos documentos, se puede encontrar para cada área las estimaciones de presupuesto, grados de incertidumbre o ambigüedad, supuestos, enfoques o metodologías según sea aplicable.

Línea base de alcance: Permite visualizar e identificar las actividades donde se presenta mayor incertidumbre con relación al manejo de la información, al igual de servir como marco para ubicar los puntos críticos de control dentro del desarrollo del proyecto.

Factores ambientales de la empresa: Se refiere a los factores tanto internos como externos de la organización que pueden impactar en el proceso. Principalmente aquellos relacionados con la estructura y cultura organizacional, el manejo de activos, políticas de personal, niveles de autoridad e infraestructura, además de la normativa existente que tenga dentro de su alcance el manejo de los sistemas de gestión de la seguridad de la información.

Activos de los procesos de la organización: Se pueden usar como entradas todos los procedimientos estandarizados que tenga la organización en relación a la seguridad de la información, listas normalizadas, plantillas, formatos, guías, instrucciones de trabajo, sistema de gestión de la documentación etc. Además de los datos históricos, lecciones aprendidas de proyectos pasados, bases de datos, niveles de autoridad.

Registro de Riesgos de seguridad de la Información: En este documento se puede encontrar la lista de los riesgos de seguridad de la información que han sido identificados, con la información que los acompaña como su posible impacto, causa raíz y responsables. De igual forma, indica

los puntos críticos de control, donde hay actividades críticas o con alta vulnerabilidad y se deben establecer controles preventivos.

Herramientas:

Juicio de Expertos: Proporciona una opinión u orientación de una persona con la experiencia y el conocimiento necesarios en seguridad de la información. Además de brindar un enfoque en el proceso de planeación, estableciendo el nivel de rigurosidad que se requiere implementar, adaptando los planes y la política de acuerdo con las necesidades del proyecto.

Reuniones: Espacios donde se haga la presentación y socialización de la política de seguridad de la información y sus respectivos planes, así como los principales controles establecidos para los procesos relacionados.

Habilidades interpersonales y de Equipo: En este proceso se necesitan habilidades como la gestión de conflictos, para alinear a los interesados con respecto a la política; facilitación para garantizar la participación de todos los interesados y el entendimiento común; Gestión de reuniones, se necesita tener una buena gestión de reuniones dada la frecuencia de estas.

Marcos de referencia: Lineamientos e indicaciones que proporcionan las guías y normativas vigentes cuyo alcance son los sistemas de gestión de la seguridad de la información. Estos proporcionan una base e Indican qué aspectos deben ser tenidos en cuenta para lograr asegurar la seguridad de la información y las definiciones normalizadas que se usan en el tema.

Salidas:

Política de seguridad de la información para la dirección del proyecto: Es un documento escrito formal, firmado y aprobado por la dirección del proyecto, donde se busca dar orientación y apoyo a la seguridad de la información teniendo en cuenta los requisitos del proyecto y la normativa aplicable. Esta política debe ser del conocimiento de todo el equipo del proyecto y si se considera necesario, de algunos interesados clave. Puede publicarse como un único documento o un conjunto de documentos relacionados.

En este documento se deben definir los objetivos y principios por los cuales se orientan todas las actividades relacionadas a la seguridad de la información, las responsabilidades y roles definidos y los procesos para manejar las desviaciones y excepciones.

El contenido y uso de esta política puede variar de acuerdo con el tamaño de la organización y el tipo de proyecto, siendo mucho más útil en organizaciones grandes y proyectos complejos o de gran envergadura.

Por lo general, una política de seguridad de la información debe contener los siguientes documentos:

- *Política de seguridad para los recursos:* Se incluyen guías para los casos de contratación, capacitación, motivación de los recursos humanos. Al igual que metodologías para controlar los demás recursos asignados al proyecto y que se vean involucrados en el proceso.

- *Política de gestión de activos de información:* Proporciona guías para hacer la clasificación y manejo de la información, de esta forma se asegura que la información importante es protegida de forma correcta. También determina reglas para el uso aceptable de los activos de información.
- *Política de seguridad de las comunicaciones*: Establece guías para asegurar la seguridad en las comunicaciones, el uso de dispositivos móviles, los procesos y medios de transferencia de información.
- *Política de gestión de vulnerabilidades*: Se define la gestión de vulnerabilidades técnicas, seguridad física y del entorno, restricciones sobre el uso de las instalaciones, software y controles de acceso. Implementación de herramientas para proporcionar seguridad a posibles códigos maliciosos.
- *Política de gestión de los incidentes de la seguridad de la información*: Proporciona unas guías a seguir en caso de incidentes, como el uso de copias de seguridad. Entre otros.
- *Política de adquisición, desarrollo y mantenimiento de sistemas de información para la Dirección del proyecto*.
- *Política de Outsourcing o Tercerización*: define los requisitos y lineamientos a seguir durante las relaciones con los proveedores y mitigar los riesgos asociados al acceso de terceros en el proyecto y que entren en contacto con los activos de información.
- *Política de tratamiento de datos personales*. Define los lineamientos necesarios para garantizar un correcto tratamiento y protección de la privacidad y los datos personales.

Controles de seguridad de la Información: Aquí se definen los controles que serán implementados para la seguridad de la información, teniendo en cuenta los puntos críticos de control, los riesgos identificados y las políticas establecidas.

Inventario de los activos de información: Documento en el que se hace un listado de todos los activos de información del proyecto y la organización. Con su respectivo número de control, descripción y características intrínsecas.

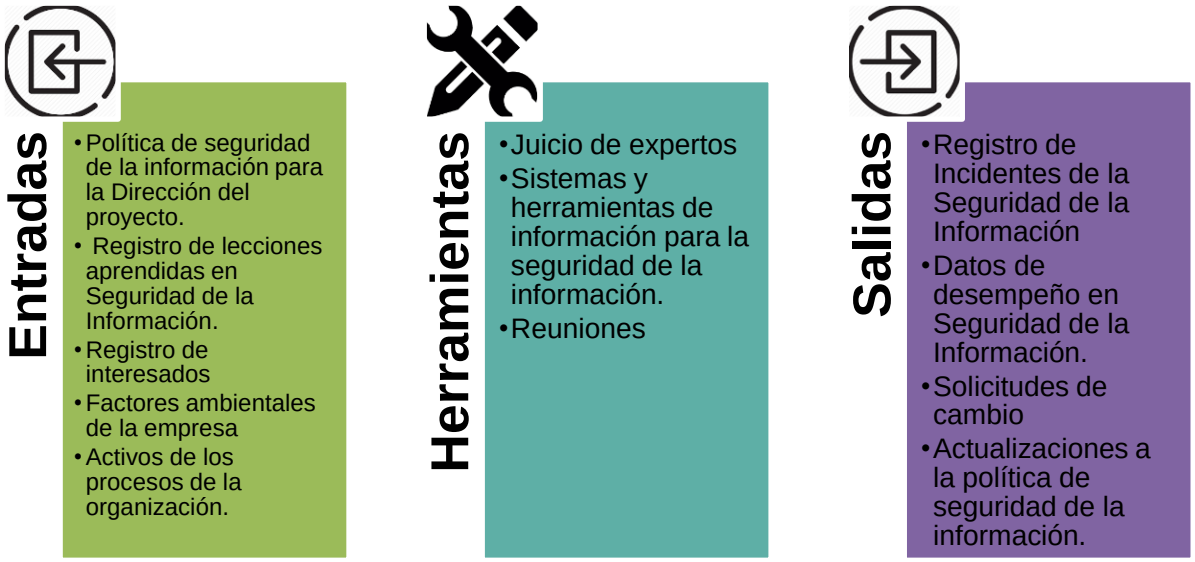
PROCESO: Implementar los controles de Seguridad de la Información

Implementar el conjunto de procedimientos y herramientas planeadas para controlar la seguridad de la información durante el proyecto, comprende las siguientes responsabilidades:

- Garantizar que durante el proyecto se ejecuten las actividades planeadas para proteger los recursos de información.
- Verificar que el plan este acorde a las necesidades de seguridad de información para el proyecto, y en efecto, solicitar cambios para realizar los ajustes respectivos.
- Implementar los cambios aprobados durante la ejecución del proyecto.
- Reunir información sobre el control de la seguridad de información durante la ejecución del proyecto.

A continuación, se presentan las entradas, herramientas y salidas de este proceso:

Figura 7.Entradas, Herramientas y Salidas para el proceso Implementar los controles de Seguridad de la Información



Entradas:

Política de seguridad de la información para la Dirección del proyecto: El conjunto de políticas, procedimientos y controles son la entrada principal para este proceso, estableciendo los lineamientos en seguridad de la información para la gestión del proyecto, con el fin de asegurar su direccionamiento y ejecución.

Registro de lecciones aprendidas en Seguridad de la información: El conocimiento adquirido por medio del registro de medidas correctivas y preventivas, que se tuvieron en la organización, en cuanto a gestión de seguridad de la información, genera una ventaja competitiva frente al tratamiento de los riesgos para mitigar el impacto en el proyecto.

Registro de Interesados: Contar con el registro de grupos, personas y organizaciones involucradas en el proyecto, permite fomentar la comunicación directa para crear conciencia de la importancia de la seguridad de la información en el proyecto.

Registro de riesgos de la seguridad de la información: Documento con el Registro de los riesgos, su valoración y puntos críticos encontrados en el proyecto, con el fin implementar los controles de seguridad para mitigar los riesgos identificados.

Factores ambientales de la empresa: Corresponde a los agentes internos de la organización que podrían aportar o entorpecer la ejecución de las políticas de seguridad de la información dentro del proyecto. En particular la cultura organizacional frente a la gestión de seguridad

Activos de los procesos de la Organización: Hace referencia a las políticas, procedimientos, herramientas y controles que se llevan a cabo dentro de la organización, o que haya trabajo en otros proyectos, para asegurar la disponibilidad, confidencialidad e integridad de la información y que puedan ayudar a la ejecución del proyecto actual.

Herramientas:

Juicio de Expertos: El conocimiento técnico en gestión para la seguridad de la información es necesario para la correcta ejecución de las políticas dentro del proyecto, aportando experiencia y experticia en la toma de decisiones.

Sistemas y herramientas de información para la seguridad de la Información: El conjunto de herramientas utilizadas para la gestión de la información dentro del proyecto depende de la organización y del proyecto. Lo importante es garantizar la seguridad y confidencialidad de la información, para la cual se pueden utilizar herramientas informáticas como: Metasploit, Nikto, John the Ripper o Nessus entre otras.

Reuniones: Durante las reuniones es muy importante asegurar la efectividad, con el fin de garantizar el abordaje de los temas pertinentes a la ejecución de los controles para la seguridad de la información en el proyecto. Se debe garantizar que la información quede plasmada en un acta con actividades de seguimiento y control.

Salidas:

Registro de incidentes de la seguridad de la información: En el numeral 6.1.6 del anexo A de la ISO 27002 menciona el aprendizaje que se obtiene de los incidentes para reducir la posibilidad e impacto de los casos futuros de quebrantamiento en la seguridad de la información. Es por esto la importancia de la identificación y registro de los incidentes de la seguridad de la información durante la ejecución del proyecto.

Solicitudes de Cambio: Las solicitudes de cambio pueden incluir acciones correctivas y preventivas en la seguridad de información para el proyecto.

Actualizaciones a la política de seguridad de la Información: En este proceso se hace relevante actualizar los documentos para registrar los eventos de seguridad y debilidades

encontradas durante la ejecución del proyecto, demostrando una realidad de las actividades que pueden alterar alguna o varias de las políticas establecidas durante el proceso de planeación.

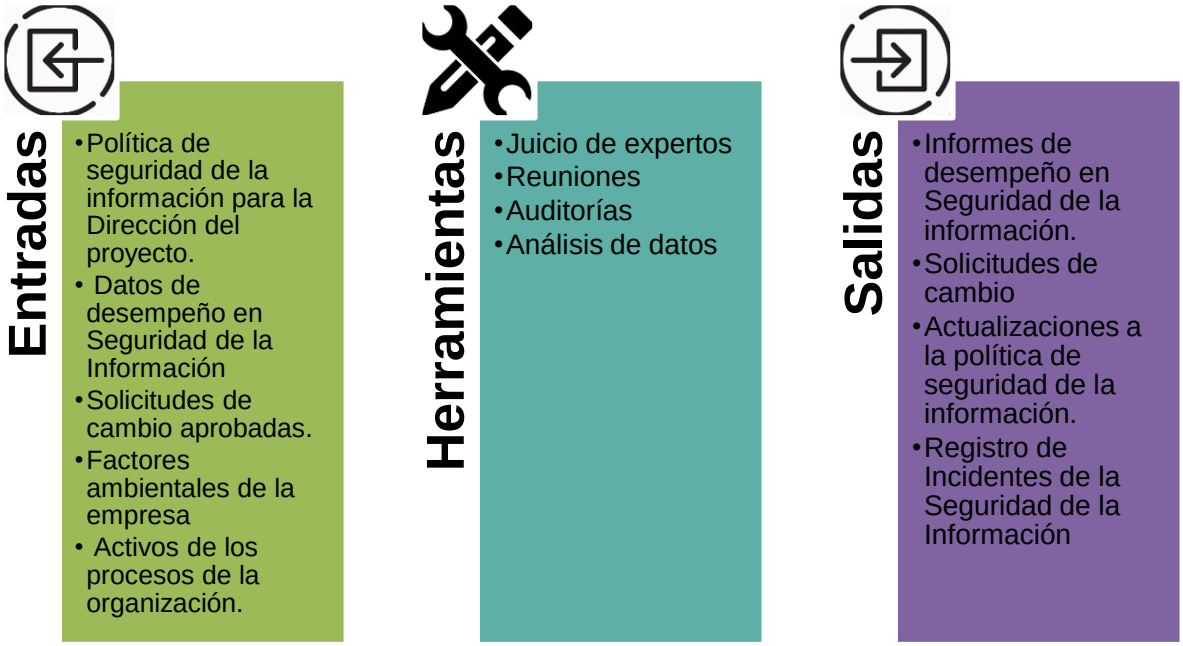
PROCESO: Monitorear los controles de Seguridad de la Información

En este proceso se debe monitorear, medir y revisar el sistema de seguridad de la información establecido para el proyecto, puede incluir alguna de las siguientes actividades:

- Gestionar los incidentes de seguridad de la información
- Revisar la eficiencia de las políticas establecidas.
- Actualizar el registro de lecciones aprendidas.
- Realizar auditorías.
- Inspeccionar que las solicitudes de cambio aprobadas están siendo acatadas.
- Revisar los niveles de los Puntos críticos de control para la seguridad de la información

Las entradas, herramientas y salidas para este proceso son:

Figura 8.Entradas, Herramientas y salidas para el proceso Monitorear los controles de Seguridad de la Información



Entradas:

Política de seguridad de la información para la dirección del proyecto: Se requieren las políticas de seguridad de la información establecidas para el proyecto, con el fin de comprobar que la ejecución se está desarrollando conforme a lo planeado, cumpliendo los objetivos planteados por la dirección del proyecto para asegurar la disponibilidad, confidencialidad e integridad de la información en el proyecto.

Datos de desempeño en seguridad de la información: Documenta las revisiones, comparando las políticas, procesos y controles planeados para la seguridad de la información con la realidad de ejecución durante el proyecto, evidenciando los resultados y toma de decisión.

Controles de seguridad de la información: Para asegurar la inspección minuciosa de los puntos críticos y riesgos identificados en la seguridad de la información del proyecto, se requiere como entrada a este proceso, los controles de seguridad plasmados durante la planeación.

Solicitudes de cambio aprobadas: Se requiere la documentación que haya modificado el plan de gestión para la seguridad de la información del proyecto, con el objetivo de verificar si los ajustes se están ejecutando.

Factores ambientales de la empresa: Factores dentro de la organización que podrían aportar o entorpecer el control en la ejecución de las políticas de seguridad de la información dentro del proyecto.

Activos de los procesos de la Organización: Hace referencia a las políticas, procedimientos, herramientas y controles que se llevan a cabo dentro de la organización, o que haya trabajo en otros proyectos, para asegurar la disponibilidad, confidencialidad e integridad de la información y que puedan ayudar a la ejecución del proyecto actual.

Herramientas:

Juicio de Expertos: Las revisiones de seguridad de la información llevada a cabo por personal experto, es un tema tratado en la ISO 27002 Anexo A, con el fin de detectar vulnerabilidades en el sistema y examinar la eficacia de los controles.

Reuniones: Intercambiar información y discutir experiencias entre el equipo de trabajo, se convierte en una herramienta útil, garantizar el seguimiento a las políticas establecidas.

Auditorías: Se llevan a cabo según la frecuencia establecida en la Política de seguridad de la información para la dirección del proyecto. Se debe evaluar el estado de los procesos, y seguimiento a los procedimientos y métodos para garantizar la seguridad de la información.

Análisis de datos: Se deben utilizar las técnicas y herramientas más apropiadas en cada caso para garantizar la seguridad de la información, ayudando a validar los datos encontrados durante el proceso de control, como medición de indicadores de cumplimiento, análisis de desempeño técnico, análisis de causa raíz, entre otros.

Salidas:

Informes de desempeño en seguridad de la información: El informe de desempeño surge como resultado de monitorear el acatamiento de las políticas, procedimientos y controles en seguridad de la información. Comunicando y evaluando la efectividad de los procesos, revisión de incidentes, amenazas y uso de accesos de vulnerabilidad.

Solicitudes de cambio: Durante el proceso de monitoreo y control, las solicitudes de cambio contrarrestan las vulnerabilidad e incidentes de seguridad de la información encontradas.

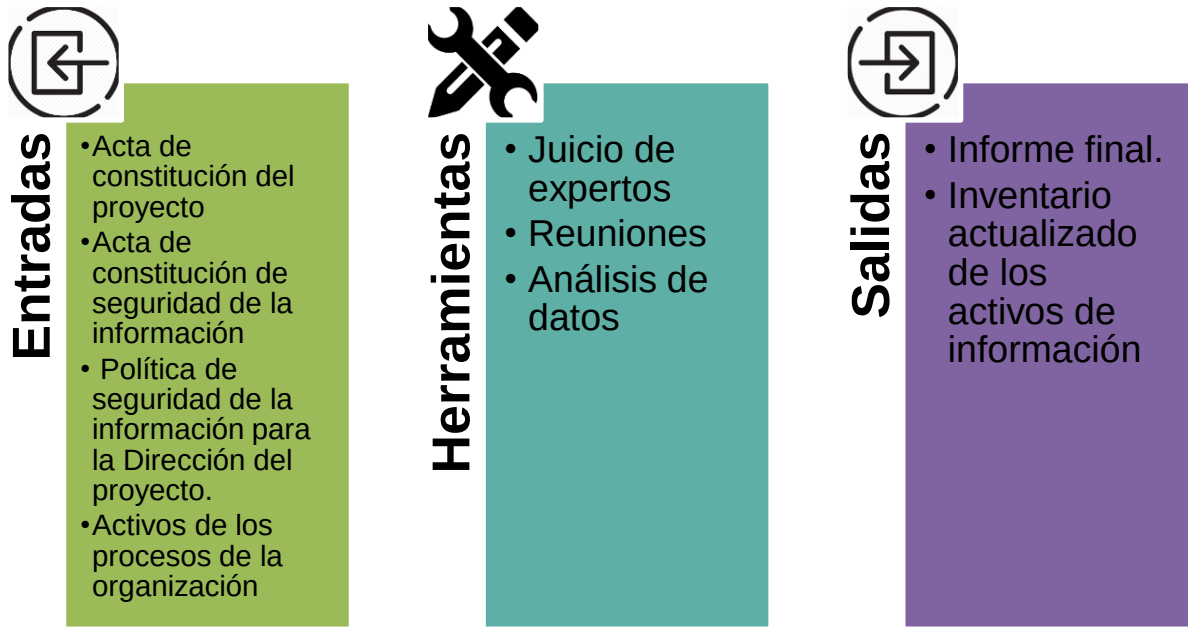
Actualizaciones a la política de seguridad de la información: Al igual que en el grupo de proceso de ejecución, este proceso actualiza las políticas para establecer, documentar y mantener sistemas seguros.

Registro de Incidentes de la seguridad de la información Debe soportar las respuestas a los incidentes, mencionando la acción inmediata, investigación del incidente y restauración de la afectación.

PROCESO: Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información.

El proceso de cerrar el uso de los controles aplicados en seguridad de la información durante el proyecto tiene como objetivo garantizar la entrega de la documentación verídica, plasmando lo sucedido durante el proyecto, además de asegurar, si es necesario, un plan de continuidad para la seguridad de la información. A continuación, se presentan las entradas, herramientas y salidas para este proceso.

Figura 9.Entradas, Herramientas y Salidas para el proceso Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información.



Entradas:

Acta de Constitución del proyecto: Documenta los criterios de aprobación inicial y final del proyecto.

Acta de constitución de seguridad de la información: Documenta los criterios generales para la planeación, ejecución, monitoreo y control y cierre de la seguridad de la información en el proyecto.

Política de Seguridad de la información para la dirección del proyecto: Se requiere demostrar que los lineamientos planeados para la seguridad de la información fueron acatados durante la gestión del proyecto.

Activos de los procesos de la Organización: Se refiere a los procesos, guías o requisitos con los que cuenta la organización para el cierre del proyecto.

Herramientas:

Juicio de Expertos: Miembros de la matriz de interesados que soporten el cierre del proyecto.

Reuniones: Las reuniones entre los interesados involucrados expertos en el cierre del uso de los controles aplicados a la seguridad de la información del proyecto, con el fin de consolidar las lecciones aprendidas, liquidaciones requeridas, además de procedimientos y controles que podrían continuar, si es necesario, una vez culminado el proyecto.

Análisis de datos: Pueden utilizarse técnicas como Análisis de documentos y Análisis de tendencias, con el fin de evaluar y validar la información registrada durante el proyecto, garantizando la seguridad de la información.

Salidas:

Informe Final: Debe contener un resumen de gestión del sistema de seguridad de la información en el proyecto. Puede incluir los siguientes documentos:

- Políticas, procedimientos y controles utilizados para garantizar la seguridad de la información.
- Resumen de incidentes.
- Indicadores de gestión y cumplimiento.
- RoadMap con los objetivos de continuidad en seguridad de la información una vez sea entregado el proyecto.
- Recomendaciones y sugerencias para garantizar la integridad, confidencialidad, disponibilidad de la información.

Inventario Actualizado de los activos de información: Como los activos de la información son cambiantes, debe entregarse un listado actualizado de estos para el cierre del proyecto, los cuales pueden encontrarse relacionados con los de la organización.

Entre ellos podemos encontrar los datos digitales, activos tangibles e intangibles, software de aplicación, sistema operativo, infraestructura y controles de TI y activos humanos, entre otros.

7. Diseño de experimento de validación.

7.1 Diseño y Aplicación

En el capítulo 5, se ha propuesto una nueva área de conocimiento dentro del marco PMBOK®, con el nombre Gestión para la seguridad de la información, enmarcados en la NTC-ISO-IEC 27002 numeral 6.1.5. Seguridad de la información en la gestión de proyectos. “La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.”

Se desarrollan 6 procesos, uno en el grupo de proceso de inicio, dos en planificación, uno en ejecución, uno en Monitoreo y uno en cierre. Cada uno de estos con sus respectivas entradas, herramientas y salidas, siguiendo el marco metodológico para la dirección de proyectos PMBOK®.

Con el objetivo de analizar la Pertinencia, coherencia, aplicabilidad y utilidad para dicha propuesta, se utiliza la herramienta de Juicio de experto, solicitando la evaluación a profesionales involucrados en el área de Dirección de proyectos y/o Seguridad de la información.

Se manejan cinco variables para medir el nivel de acuerdo o desacuerdo, donde la más baja calificación es totalmente en desacuerdo, seguido por, desacuerdo, el intermedio esta evaluado por la frase, ni de acuerdo ni en desacuerdo, el cuarto nivel es, de acuerdo y la mayor puntuación es totalmente de acuerdo. La encuesta es diseñada y enviada por medio de la herramienta de formularios de Google ®. Ver Anexo D, Respuestas de la validación.

7.2 Resultados

Se hace evidente en el proceso de validación que los expertos están de acuerdo con el hecho de la necesidad de incluir en el marco metodológico la seguridad de la información como proceso, sin embargo, se refleja un alto nivel de desacuerdo en el hecho de incluir una nueva área de conocimiento.

Identificar y valorar los riesgos, planificar los controles e implementar los controles de la seguridad de la información, son los procesos con mayor aceptación dentro del juicio de experto, evidenciando la necesidad de garantizar que los riesgos asociados a esta deben ser tenidos en cuenta durante todo el proyecto, resaltando una metodología de riesgo como entrada de los procesos. No obstante, el proceso de desarrollar un acta de cierre del uso de los controles aplicados de seguridad de la información tiene mayor índice de rechazo, argumentando el entorpecimiento al cierre del proyecto.

Con el fin de garantizar la disponibilidad, confidencialidad e integridad de la información durante la dirección de proyectos se presenta como sugerencia incluir algunos procesos dentro de las 10 áreas existentes o incluso dentro de los procesos existentes.

Conclusiones y futuro trabajo

- La primera herramienta desarrollada cumple con proporcionar información exploratoria sobre la percepción general de los encuestados en relación a los marcos de trabajo para la dirección de proyectos y para la seguridad de la información.

- La segunda Herramienta que se desarrolla, cumple con proporcionar información más específica sobre el grado de manejo de los marcos de trabajos en dirección de proyectos y el uso de la seguridad de la información durante el desarrollo de los mismos.

- A pesar de que las empresas encuestadas declaran conocer y aplicar buenas prácticas en dirección de proyectos y la mayoría coincidió en que es importante poder garantizar al cliente la disponibilidad, confidencialidad e integridad de la información, menos de la mitad reconoce o aplica las medidas de gestión de seguridad de la información recomendadas por marcos teóricos como la ISO/IEC 27001 Anexo A o ISO/IEC 27002. Además, indican que los principales obstáculos para implementar las medidas de dichas normas son el costo y tiempo para hacerlo.

- Los encuestados en la segunda fase, aplican marcos para la gestión de proyectos y usan las técnicas de gestión de riesgos, sin embargo, no identifican los riesgos de seguridad de la información dentro del proyecto ni cuentan con políticas o procedimientos que soporten la gestión de medidas para garantizar la disponibilidad, confidencialidad e integridad de la información.

- Los resultados de las encuestas demostraron un bajo uso de las técnicas de gestión de seguridad de la información, por lo cual se propuso la inclusión de una nueva área del conocimiento en el marco de trabajo para la dirección de proyectos del PMBOK®, esperando brindar una guía clara para la implementación de las medidas de seguridad de la información en el desarrollo del proyecto y fomentar su uso.

- Se propone en trabajos futuros realizar de nuevo un sondeo con un número de muestra más grande o incluyendo empresas de otros sectores que manejen proyectos para ellos o sus clientes. De esta forma se puede ampliar la comprensión sobre el estado actual del uso de metodologías de gestión de la seguridad de la información en las organizaciones.

- De acuerdo con los resultados obtenidos en el proceso de validación de la propuesta, se recomienda en futuros trabajos, analizar en qué áreas de conocimiento se podrían introducir los procesos para la gestión de seguridad de la información, con el fin de mantener las 10 áreas existentes en el marco de trabajo del PMBOK®.

- En futuros trabajos también se puede proponer la inclusión de técnicas y herramientas de trabajo de gestión de seguridad de la información en otros marcos de trabajo para la dirección de proyectos existentes.

- Como consecuencia de las observaciones recibidas durante el proceso de Validación, se adaptó una nueva entrada en el proceso de Identificar y valorar los riesgos de seguridad de la información, llamada Metodología de Riesgos.

- Como trabajo futuro se propone generar herramientas digitales y automatizadas para las salidas de los procesos planteados, pueden ser utilizados programas especiales desarrollados o programas existentes como Excel, con el fin de soportar los procesos y procedimientos para controlar la seguridad de la información.

Bibliografía

Cortes, J. F. (2015). Seguridad de la Información en pequeñas y medianas empresas (Pymes). Universidad Piloto de Colombia.

DANE. (s.f.). CLASIFICACIÓN INDUSTRIAL INTERNACIONAL UNIFORME DE TODAS LAS ACTIVIDADES ECONÓMICAS. *Revisión 4 adaptada para Colombia*.

Esteban, I. G., & Fernández, E. A. (2014). *Fundamentos y Técnicas de Investigación Comercial.* Madrid: Gráficas Dehon.

ISO/IEC 27001 Anexo A. (Septiembre de 2013). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*.

ISO/IEC 27002. (Septiembre de 2013). *Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información*.

Lowe, S. (17 de Mayo de 2016). *PM Times Resources for Project Managers.* Obtenido de Information Security Project Management: https://www.projecttimes.com/articles/information-security-project-management.html

MINTIC. (6 de Noviembre de 2016). Guía para la Implementación de Seguridad de la Información en una MIPYME.

Monteiro, A., Santos, V., & Varajao, J. (2016). Project Management Office Models - A Review. *Elsevier*, 10.

Muñoz, I. L. (2018). *Preparación Efectiva Para el Examen PMP-CAMP.* Cali: Domuz.

Project Management Institute. (2017). *A guide to the project management body of knowledge (pmbok® guide)–sixth edition.* Project Management Institute.

Reyes, E., & Polonia, E. D. (13 de Enero de 2013). Guía de Seguridad Para Información Pymes. Machiques, Venezuela: Instituto Universitario de Tecnología de Maracaibo.

Anexos

Anexo A. Herramienta encuesta grado básico

Encuesta academica en busca del desarrollo de nuestra región en la gestión de proyectos y seguridad de la información.

Somos estudiantes de la maestría en Gerencia de proyectos de la Universidad Icesi. Estamos explorando el uso de buenas prácticas en los proyectos y seguridad de la información en las miPymes del sector informática y comunicaciones de la ciudad de Cali, para lo cual agradecemos nos colabore respondiendo las 8 preguntas en el formulario adjunto, o en su defecto enviando al área o persona encargada del manejo de proyectos en su empresa, esto tardará máximo 1 minuto de su tiempo. Muchas gracias por su colaboración.

*Obligatorio

Dirección de correo electrónico *

Tu dirección de correo electrónico

Sobre la gerencia de proyectos.

1. ¿Su organización desarrolla proyectos para sus clientes? *

- ○ Si
- ○ No
- ○ Algunas Veces

2. ¿En su organización utilizan alguno de estos marcos metodológicos para la gestión de proyectos? *

- [ ] PMBOK
- [ ] SCRUM
- [ ] PRINCE
- [ ] ASAP
- [ ] METODOS AGILES
- [ ] Ninguno
- [ ] Otro: _____

3. ¿En su organización cuentan con una herramienta tecnológica para soportar los proyectos de sus clientes? *

- ○ SI
- ○ No

4. ¿Cuenta con roles capacitados en administración de proyectos para liderar los proyectos de sus clientes? *

- ○ Sí
- ○ No

Sobre la seguridad de la información.

5. ¿Sus clientes requieren que usted les garantice la disponibilidad, confidencialidad e integridad de la información del proyecto que usted gestiona para ellos? *

- ○ Sí
- ○ No

6. ¿En su organización utilizan alguno de estos marcos de Seguridad de la Información o riesgos? *

- [ ] ISO27001
- [ ] ISO27002
- [ ] ISO31000
- [ ] Ninguno
- [ ] Otro: _____

7. ¿En su organización cuentan con una herramienta tecnológica para soportar el sistema de gestión de seguridad de la información de sus clientes? *

- ( ) Sí
- ( ) No

8. A su juicio ¿Cuál es el principal obstáculo en su organización para no contar con buenas prácticas de proyectos y sistema de gestión de seguridad de la información que le permitan lograr obtener la rentabilidad requerida? *

- [ ] Tiempo de dedicación para la implementación.
- [ ] Costo de inversión para el acompañamiento
- [ ] Falta de talento humano o personal de apoyo
- [ ] No es necesario
- [ ] Otro: _____

Anexo B. Herramienta encuesta grado intermedio

Encuesta de profundización académica en busca del desarrollo de nuestra región en la gestión de proyectos y seguridad de la información.

Agradecemos su participación en nuestro proyecto educativo, en esta fase de profundización lograremos una visual clara pero sencilla sobre el nivel de involucramiento de su empresa en la ejecución de buenas prácticas en los proyectos y seguridad de la información.

Esto tardará máximo 5 minutos de su tiempo. Muchas gracias por su colaboración.

Su participación en este proceso le permitirá recibir de vuelta los resultados generales que obtengan las miPymes participantes del sector informática y comunicaciones de la ciudad de Cali, sin mencionar nombres de empresas.

*Obligatorio

Dirección de correo electrónico *

Tu dirección de correo electrónico

Sobre la gerencia de proyectos predictivos.

1. ¿Los proyectos que ejecuta su organización tienen objetivos claros y medibles, además de alcance, tiempo, costo y calidad? *

- ○ siempre
- ○ Casi siempre
- ○ Algunas Veces
- ○ Nunca

2. ¿Su organización utiliza y mantiene un marco de referencia de trabajo con metodología y procesos de administración de proyectos común para todos sus proyectos? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas Veces
- ○ Nunca

3. Para iniciar un proyecto en su organización el responsable: *

- ○ Presenta verbalmente en una reunión la descripción del alcance y los propósitos generales del proyecto al patrocinador.
- ○ Presenta al patrocinador un documento breve, cuyo contenido depende de la iniciativa de cada persona.
- ○ Entrega al patrocinador un documento que la organización tiene preparado para esta etapa de los proyectos. Teniendo en cuenta las características de justificación, alcance, tiempo y costo.
- ○ Otro:

4. ¿Al inicio de los proyectos se identifican todas las personas, contratistas, clientes, usuarios, etc., que se verán afectados o involucrados en cualquier etapa del proyecto? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

5. ¿Su organización maneja hitos definidos, donde se evalúan los entregables de proyecto para determinar si se debe continuar o terminar? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

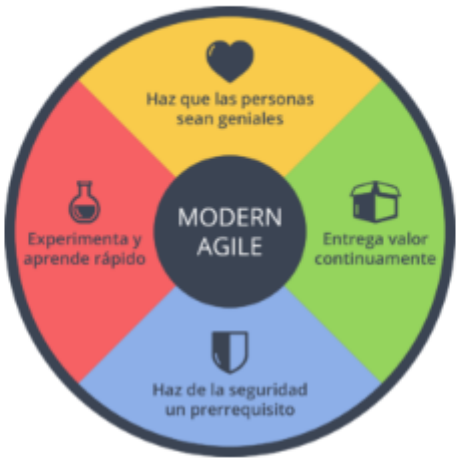
6. ¿Su organización utiliza técnicas de gestión del riesgo para medir y evaluar el impacto del riesgo durante la ejecución de los proyectos? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

7. La aprobación de un Plan de proyecto en su organización contempla: *

- ○ Cronograma.
- ○ Cronograma y presupuesto
- ○ Cronograma, presupuesto, alcance y riesgos.
- ○ Lo mencionado en el punto anterior más planes subsidiarios de comunicaciones, recursos entre otros.

Sobre la gerencia de proyectos Ágiles.



8. ¿Los proyectos que ejecuta la organización hacen hincapié en la entrega temprana y frecuente de las salidas del proyecto? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

9. ¿Considera que los proyectos que ejecuta su organización se desglosan en entregables que agregan valor de manera inmediata? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

10. ¿Considera que los proyectos en su organización tienen ciclos de retroalimentación por parte de los clientes? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

11. ¿La organización le apuesta a proyectos de alta incertidumbre? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

12. ¿En los proyectos de su organización hay oportunidades de productos mínimos viables o de elaboración de prototipos? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

13. ¿En su organización el equipo de proyecto planifica y replanifica a medida que se obtiene más información a partir de entregas frecuentes? *

- ○ Siempre
- ○ Casi siempre
- ○ Algunas veces
- ○ Nunca

Sobre la seguridad de la información

1. ¿Cuenta su organización con un organigrama definido y estandarizado? *

- ○ Sí
- ○ No

2. ¿Cuenta con un mapa de procesos estandarizado para la organización? *

- ○ Sí
- ○ No

3. ¿Cuenta con alguna política de seguridad de la información y/o ciberseguridad aprobada y divulgada formalmente dentro de la organización. *

- ○ Sí
- ○ No

4. ¿Cuenta con un inventario actualizado y clasificado de acuerdo a la criticidad de los activos de información de la organización? *

- ○ Sí
- ○ No

5. ¿Su organización tiene un esquema de clasificación de la información (ejemplo: publico, semiprivado, privado, sensible -1581)? *

- ○ Sí
- ○ No

6. ¿Cuenta la organización con alguna metodología de riesgos estandarizada? *

- ○ Sí
- ○ No

7. ¿La organización tiene identificado a que riesgos de seguridad de la información están expuestos los activos de información? *

- ○ Sí
- ○ No

8. ¿Cuenta con un esquema de roles y responsabilidades en seguridad de la información definida en la organización? *

- ○ Sí
- ○ No

9. ¿Su organización actualmente cuenta con un plan de continuidad del negocio y/o recuperación de desastres? *

- ○ Sí
- ○ No

10. ¿Cuenta con procedimientos, lineamientos e instructivos de seguridad de la información documentados y divulgados dentro de la organización (ejemplo, procedimiento de gestión de incidentes en seguridad de la información.? *

- ○ Sí
- ○ No

Anexo C. Herramienta validación de la nueva área de conocimiento en la dirección de proyectos

Seguridad de la Información en la Dirección de Proyectos

Para nuestro trabajo de grado hemos propuesto una nueva área de conocimiento dentro del marco PMBOK, a la cual llamamos Gestión para la seguridad de la información, enmarcados en la NTC-ISO-IEC 27002 numeral 6.1.5. Seguridad de la información en la gestión de proyectos. "La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto."

Se desarrollaron 6 procesos, uno en el grupo de proceso de inicio, dos en planificación, uno en ejecuciòn, uno en Monitoreo y uno en cierre.

Cada uno de estos con sus respectivas entradas, herramientas y salidas, siguiendo el marco metodológico para la dirección de proyectos PMBOK.

Con el objetivo de analizar la Pertinencia, coherencia, aplicabilidad y utilidad para dicha propuesta, utilizamos la herramienta de Juicio de experto, por lo que solicitamos su evaluación como conocedor en el área de Dirección de proyectos y/o Seguridad de la información.
Se están manejando cinco variables, donde 1 o la mas baja calificación es totalmente en desacuerdo, 2 es en desacuerdo, 3 es ni de acuerdo ni en desacuerdo, 4 es de acuerdo y 5 es la mayor puntuación o totalmente de acuerdo.

*Obligatorio

Propuesta àrea de conocimiento - Gestión de la Seguridad de la información del Proyecto.

Área de Conocimiento	Grupo de Procesos de la Dirección de Proyectos				
	Grupo de procesos de Inicio	Grupo de procesos de Planeación	Grupo de procesos de Ejecución	Grupo de procesos de Monitoreo y control	Grupo de procesos de Cierre
Gestión de la Seguridad de la información del Proyecto	- Desarrollar el acta de constitución frente a la seguridad de la información.	- Identificar y Valorar los riesgos de seguridad de la información. - Planificar los controles de Seguridad de la Información.	-Implementar los controles de Seguridad de la Información.	- Monitorear los controles de Seguridad de la Información.	- Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información.

¿Estas de acuerdo o en desacuerdo con incluir el área de conocimiento "Gestión de la Seguridad de la información del proyecto"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

Grupo de Proceso de Inicio

Proceso - Desarrollar el acta de constitución frente a la seguridad de la información

En este proceso se desarrolla el acta de constitución frente a la seguridad de la información, donde se describen y presentan formalmente el alcance, los límites y lineamientos generales que tendrá la gestión de la seguridad de la información durante el proyecto. Aquí el patrocinador da su aprobación y las partes se comprometen a asegurar la seguridad de la información durante el proyecto.

¿Estas de acuerdo o en desacuerdo con el proceso "Desarrollar el acta de constitución frente a la seguridad de la información"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

Observaciones

Déjenos saber si tiene comentarios adicionales sobre este nuevo proceso.

Tu respuesta

Grupo de Proceso de Planeaciòn

Proceso - Identificar y Valorar los riesgos de seguridad de la información

En este proceso se determinan y documentan los riesgos individuales sobre la seguridad de la información, se describen las causas, responsables y posibles respuestas. Se saca una lista de amenazas y oportunidades que pueden impactar a los activos de la información, la comunicación y la confidencialidad, disponibilidad e integridad de datos.

También se incluye una valoración cualitativa de los riesgos identificados, evaluando y combinando la probabilidad de ocurrencia y el impacto de dichos riesgos.
En este documento se incluye la identificación de los puntos críticos de control que se deben ser marcados en el ciclo de vida del proyecto, teniendo en cuenta que en éstos es donde se deben implementar controles preventivos y de seguridad.
Este proceso es iterativo, ya que los riesgos sobre la seguridad de la información y los posibles puntos de control pueden ser identificados a medida que se desarrolla el proyecto y es necesario actualizar las listas

¿Estas de acuerdo o en desacuerdo con el proceso "Identificar y Valorar los riesgos de seguridad de la información"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

Observaciones

Grupo de Proceso de Planeaciòn

Proceso - Planificar los controles de Seguridad de la Información

En este proceso se desarrolla un documento o una serie de documentos relacionados donde se define la política de seguridad de la información que se usará para la dirección del proyecto. Aquí se definen los objetivos y principios por los cuales se orientan todas las actividades del proyecto que estén relacionadas a la seguridad de la información.
De esta forma, se emite de forma centralizada una directriz firmada por la alta dirección que debe ser conocida por todas las partes del proyecto y los interesados externos para los cuales se defina la necesidad.

¿Estas de acuerdo o en desacuerdo con el proceso "Planificar los controles de Seguridad de la Información"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

Observaciones

Déjenos saber si tiene comentarios adicionales sobre este nuevo proceso.

Tu respuesta

Grupo de Proceso de Ejecuciòn

Proceso - Implementar los controles de Seguridad de la Información

Implementar el conjunto de procedimientos y herramientas planeadas para controlar la seguridad de la información durante el proyecto, comprende las siguientes responsabilidades:

- Garantizar que durante el proyecto se ejecuten las actividades planeadas para proteger los recursos de información.
- Verificar que el plan este acorde a las necesidades de seguridad de información para el proyecto, y en efecto, solicitar cambios para realizar los ajustes respectivos.
- Implementar los cambios aprobados durante la ejecución del proyecto.
- Reunir información sobre el control de la seguridad de información durante la ejecución del proyecto.

¿Estas de acuerdo o en desacuerdo con el proceso "Implementar los controles de Seguridad de la Información"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

Observaciones

Déjenos saber si tiene comentarios adicionales sobre este nuevo proceso.

Grupo de Proceso de Monitoreo y Control

Proceso - Monitorear los Controles de seguridad de la Información

En este proceso se debe monitorear, medir y revisar el sistema de seguridad de la información establecido para el proyecto, puede incluir alguna de las siguientes actividades:

- Gestionar los incidentes de seguridad de la información
- Revisar la eficiencia de las políticas establecidas.
- Actualizar el registro de lecciones aprendidas.
- Realizar auditorías.
- Inspeccionar que las solicitudes de cambio aprobadas están siendo acatadas.
- Revisar los niveles de los Puntos críticos de control para la seguridad de la información

¿Estas de acuerdo o en desacuerdo con el proceso "Monitorear los Controles de seguridad de la Información"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

Observaciones

Grupo de Proceso de Cierre

Proceso - Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información

El proceso de cerrar el uso de los controles aplicados en seguridad de la información durante el proyecto tiene como objetivo garantizar la entrega de la documentación verídica, plasmando lo sucedido durante el proyecto, además de asegurar, si es necesario, un plan de continuidad para la seguridad de la información. A continuación, se presentan las entradas, herramientas y salidas para este proceso.

¿Estas de acuerdo o en desacuerdo con el proceso "Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información"? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Pertinencia	○	○	○	○	○
Coherencia	○	○	○	○	○
Aplicabilidad	○	○	○	○	○
Utilidad	○	○	○	○	○

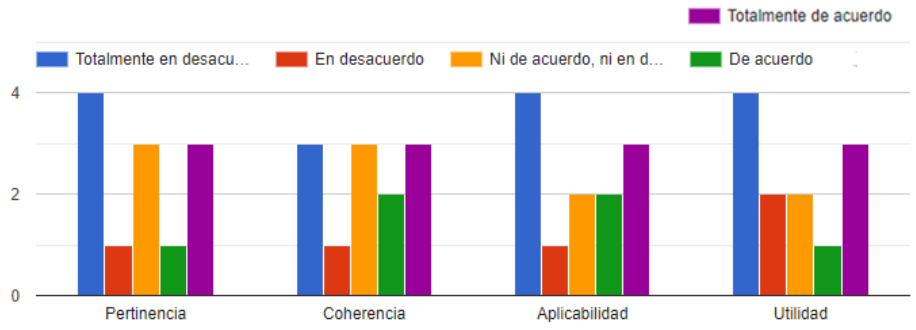
Observaciones

Déjenos saber si tiene comentarios adicionales sobre este nuevo proceso.

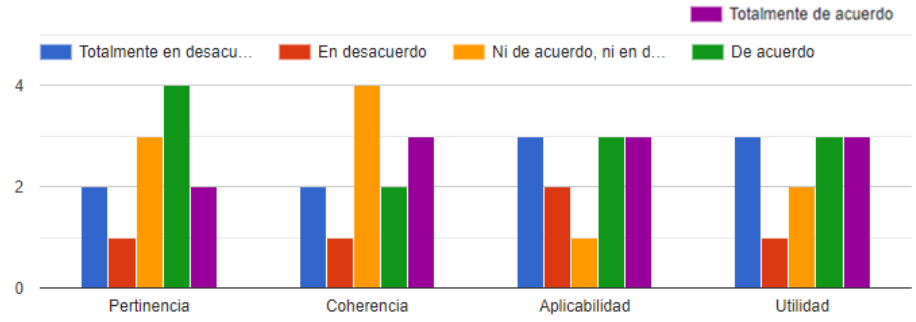
Tu respuesta

Anexo D. Resultados encuesta validación de la nueva área de conocimiento en la dirección de proyectos

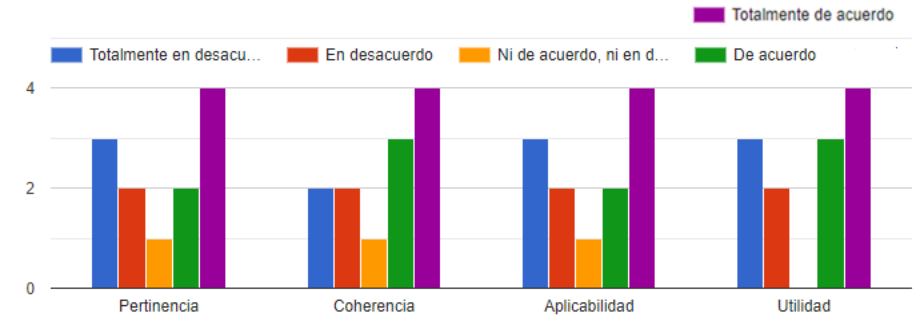
¿Estas de acuerdo o en desacuerdo con incluir el área de conocimiento "Gestión de la Seguridad de la información del proyecto"?



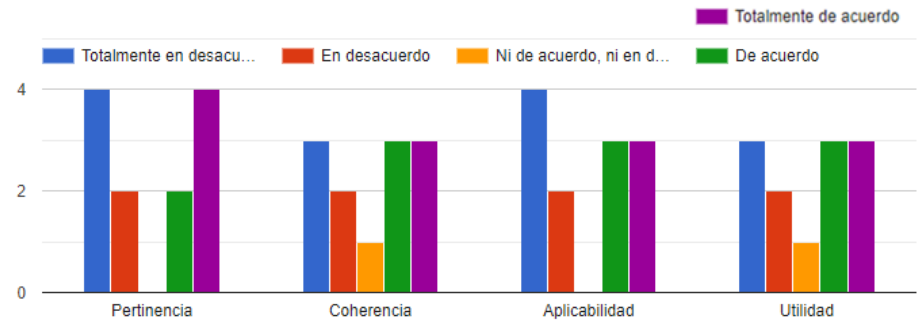
¿Estas de acuerdo o en desacuerdo con el proceso "Desarrollar el acta de constitución frente a la seguridad de la información"?



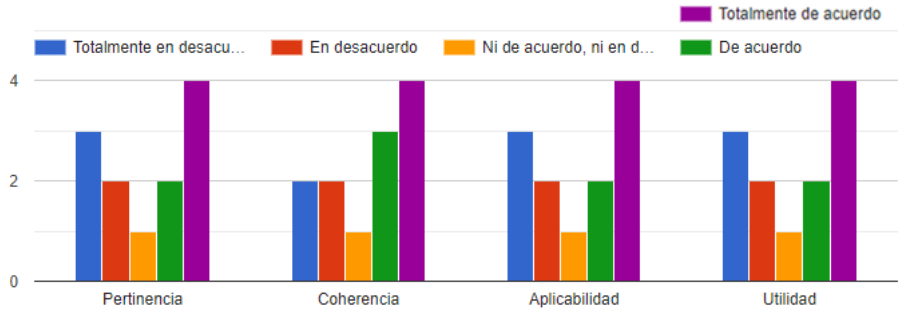
¿Estas de acuerdo o en desacuerdo con el proceso "Identificar y Valorar los riesgos de seguridad de la información"?



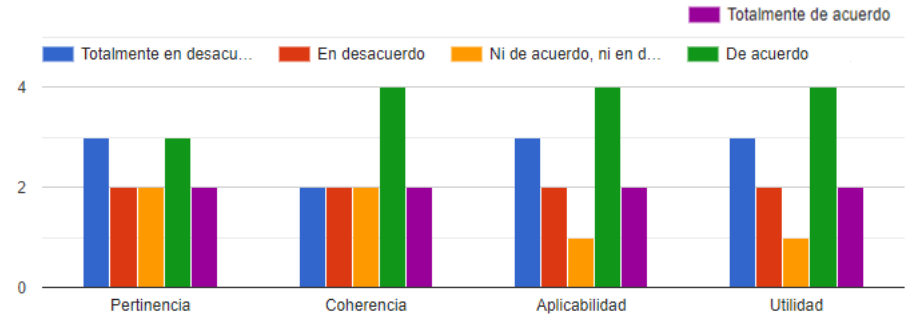
¿Estas de acuerdo o en desacuerdo con el proceso "Planificar los controles de Seguridad de la Información"?



¿Estas de acuerdo o en desacuerdo con el proceso "Implementar los controles de Seguridad de la Información"?



¿Estas de acuerdo o en desacuerdo con el proceso "Monitorear los Controles de seguridad de la Información"?



¿Estas de acuerdo o en desacuerdo con el proceso "Desarrollar acta de cierre del uso de los controles aplicados de Seguridad de la Información"?