

NEUMANN BUSINESS SCHOOL
ESCUELA DE POSTGRADO

**MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS
DE LA INFORMACIÓN**



**“ESTUDIO DEL DESEMPEÑO DE MECANISMOS
DE SEGURIDAD DE LA INFORMACIÓN EN
EMPRESAS MINERAS. EL CASO DE UNA EMPRESA
MINERA EN EL SUR DEL PERÚ – 2019”**

TESIS PARA OPTAR EL GRADO A NOMBRE DE LA NACIÓN DE:

**MAESTRO EN GESTIÓN DE TECNOLOGÍAS
DE LA INFORMACIÓN**

AUTOR:

IVÁN VICTOR ALVARADO ESPEJO

DOCENTE GUÍA:

LUIS ENRIQUE ESPINOZA VILLALOBOS

**TACNA - PERÚ
2020**

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

INDICE DE CONTENIDO

	Pág.
RESUMEN EJECUTIVO	i
INTRODUCCIÓN	iii
CAPÍTULO I	
ANTECEDENTES DE ESTUDIO	1
1.1 Título del tema	1
1.2 Planteamiento del problema	1
1.3 Formulación del problema	3
1.3.1 Problema general	3
1.3.2 Problemas específicos	3
1.4 Hipótesis	3
1.4.1 Hipótesis general	3
1.1.1. Hipótesis específicas	4
1.5 Objetivos	4
1.5.1 Objetivo general	4
1.5.2 Objetivos específicos	4
1.6 Justificación.	5
1.7 Metodología	5
1.8 Definiciones	6
1.8 Alcances y limitaciones	9
CAPÍTULO II	
MARCO TEÓRICO	11
2.1 Conceptualización de la variable independiente.....	11
2.1.1 Mecanismo de seguridad según x800	11
2.1.2 COBIT	20
2.1.3 ITIL	22
2.1.4 Amenazas de seguridad.....	26
2.1.5 Servicios de seguridad	30
2.1.6 Clases de mecanismos de seguridad	37
2.1.7 Tipos de mecanismos de seguridad	42
2.2 Importancia de la variable independiente	45
2.3 Modelo de evaluación de la variable independiente	45
2.4 Conceptualización de la variable dependiente 1	46
2.4.1 Diseño de sistemas	46
2.4.2 Sistemas interactivos	57
2.4.3 Medidas orientadas al usuario.....	62
2.4.4 Formación de los usuarios	64
2.4.5 Recursos humanos y TI	67
2.4.6 Computación del usuario final	70
2.4.7 Implicación e influencia del usuario	75
2.4.8 Satisfacción del usuario	78
2.5 Importancia de la variable dependiente 1	80
2.6 Modelo de evaluación de la variable dependiente 1	81
2.7 Conceptualización de la variable dependiente 2.....	82
2.7.1 Planificación de sistemas	83
2.7.2 Sistemas y mecanismos.....	87
2.7.3 Metodología de selección.....	89
2.7.4 Sistemas y planificación	90
2.7.5 Planificación estratégica de SI	97

2.7.6	Funciones gerenciales	99
2.7.7	Compromiso administrativo	106
2.8	Importancia de la variable dependiente 2	111
2.9	Modelo de evaluación de la variable dependiente 2	112
2.10	Análisis comparativo	113
2.11	Análisis crítico	114
CAPÍTULO III		
MARCO REFERENCIAL		115
3.1	Reseña histórica	115
3.2	Misión y visión.....	116
3.3	Valores.....	116
3.4	Desempeño operativo	117
3.5	Gestión social.....	120
3.6	Gestión ambiental	122
3.7	Gestión del agua	123
3.8	Gestión de residuos	124
3.9	Gestión de emisiones.....	125
3.10	Gestión de energía.....	127
3.11	Diagnóstico sectorial	127
3.11.1	Poder de negociación con proveedores	128
3.11.2	Poder de negociación de los clientes	129
3.11.3	Amenaza de nuevos competidores	130
3.11.4	Amenaza de productos o servicios sustitutos.....	130
3.11.5	Rivalidad entre los competidores existentes.....	131
CAPÍTULO IV		
RESULTADOS		132
4.1	Mecanismos de SI implementados.....	132
4.2	Marco Metodológico	143
4.2.1	Instrumentos	144
4.3	Tipo de diseño.....	150
4.4	Población	150
4.5	Muestra	151
4.6	Recolección de información	152
4.7	Resultados para la variable D1	153
4.7.1	Validación y confiabilidad del instrumento	153
4.7.2	Diseño de presentación de datos	156
4.8	Resultados para la variable D2	162
4.8.1	Validación y confiabilidad del instrumento	162
4.8.2	Diseño de presentación de datos	165
4.9	Resultados para la variable independiente.....	171
4.9.1	Validación y confiabilidad del instrumento	171
4.9.2	Diseño de presentación de datos	174
4.10	Contraste de hipótesis.....	178
CONCLUSIONES		186
SUGERENCIAS		187
BIBLIOGRAFIA		188
ANEXOS.....		190

INDICE DE TABLAS

	Pág.
Tabla N° 1 Operacionalización de la variable independiente	07
Tabla N° 2 Operacionalización de la variable dependiente PU.....	08
Tabla N° 3 Operacionalización de la variable dependiente PS	09
Tabla N° 4 Mecanismos específicos de seguridad	12
Tabla N° 5 Mecanismos generales de seguridad.....	13
Tabla N° 6 Relación entre servicios de seguridad y ataques	14
Tabla N° 7 Relación entre servicios y mecanismos de seguridad.....	15
Tabla N° 8 Servicios de seguridad por nivel OSI según la norma ISO 7496.....	40
Tabla N° 9 Clasificación de la variable independiente	45
Tabla N° 10 Pasos en la especificación de usuarios destinatarios del sitio web.....	54
Tabla N° 11 Explicación de ciertos procesos de la ingeniería de usabilidad.....	56
Tabla N° 12 Recursos humanos del SI y sus competencias.....	67
Tabla N° 13 Preocupaciones típicas de los usuarios y especialistas técnico.....	77
Tabla N° 14 Clasificación de la variable dependiente PU	81
Tabla N° 15 Clasificación de la variable dependiente PS	112
Tabla N° 16 Indicadores de producción	118
Tabla N° 17 Reservas de la UM Pucamarca.....	119
Tabla N° 18 Extracción de agua por fuente	124
Tabla N° 19 Residuos peligrosos y no peligrosos por tipo de eliminación	125
Tabla N° 20 Variación de las emisiones por unidad.....	126
Tabla N° 21 Consumo total de energía (GJ)	127
Tabla N° 22 Variables – Indicadores – Ítems - Mecanismos.....	133
Tabla N° 23 Formato de especificación de requerimiento.....	137
Tabla N° 24 Descripción de indicadores	146
Tabla N° 25 Preguntas por indicador	147
Tabla N° 26 Variables, indicadores e ítems	149
Tabla N° 27 Estratos de población.....	150
Tabla N° 28 Estratos de muestra	152
Tabla N° 29 Resultados de la validación de los ítems PU	155
Tabla N° 30 Estadístico de confiabilidad.....	155
Tabla N° 31 Alfa de Cronbach	156
Tabla N° 32 Participación en el uso de herramientas de SI de su empresa	157
Tabla N° 33 Participación En La Seguridad De Los Sistemas	158
Tabla N° 34 Participación en la identificación del riesgo en TI.....	159
Tabla N° 35 Participación en proyectos tecnológicos	160
Tabla N° 36 Participación en la ejecución de pruebas de control	161
Tabla N° 37 Resultados de la validación de los ítems PS.....	164
Tabla N° 38 Estadístico de confiabilidad.....	164
Tabla N° 39 Alfa de Cronbach	165
Tabla N° 40 Control al sistema de información	166
Tabla N° 41 Control de recursos de infraestructura tecnológica	167
Tabla N° 42 Control de recursos de software	168

Tabla N° 43 Metodología de implementación	169
Tabla N° 44 Estrategia del sistema de información	170
Tabla N° 45 Resultados de la validación de los ítems PS.....	173
Tabla N° 46 Estadístico de confiabilidad.....	173
Tabla N° 47 Alfa de Cronbach	174
Tabla N° 48 Control al sistema de información	175
Tabla N° 49 Segregación de funciones en el sistema de información	176
Tabla N° 50 Políticas de seguridad y acceso al sistema.....	177
Tabla N° 51 Correlación de Spearman	179
Tabla N° 52 Correlación de Spearman	182

ÍNDICE DE FIGURAS

Figura N° 1 Modelo para la seguridad de redes.....	18
Figura N° 2 Modelo para la seguridad en el acceso a redes.....	19
Figura N° 3 Pentágono de Gobierno de TI.....	21
Figura N° 4 Marco para la gestión de seguridad de TI.....	22
Figura N° 5 Controles de seguridad para amenazas e incidencias.....	24
Figura N° 6 Agresiones a la seguridad de red activas y pasivas	27
Figura N° 7 Antivirus, seguridad lógica	33
Figura N° 8 Firma digital	33
Figura N° 9 Detector de humos.....	34
Figura N° 10 Sistema de alimentación ininterrumpida	35
Figura N° 11 Mecanismos y servicios de seguridad	36
Figura N° 12 Mecanismos de hardware	43
Figura N° 13 Tarjeta para el control de acceso	43
Figura N° 14 Sistema de acondicionamiento de aire	44
Figura N° 15 Distribución de documentos relevantes	63
Figura N° 16 Niveles de satisfacción del usuario	80
Figura N° 17 Características de un proyecto planificado	84
Figura N° 18 Sistema genérico	91
Figura N° 19 Tipo de estructura de un sistema.....	92
Figura N° 20 Planificación dentro de la administración de proyectos	93
Figura N° 21 Proceso de Planificación.....	96
Figura N° 22 Evolución de la planificación estratégica de sistemas	98
Figura N° 23 Relación entre las áreas y procesos de planeación.....	100
Figura N° 24 Transformación de conjuntos de estrategias	102
Figura N° 25 Influencia entre procesos de planificación	102
Figura N° 26 Marco de referencia de un plan de recursos de información	103
Figura N° 27 Ejemplo de plan estratégico de un sistema de inventarios	105
Figura N° 28 Valores de la empresa	116
Figura N° 29 Cash cost por tonelada tratada	118
Figura N° 30 Programas de desarrollo social.....	121
Figura N° 31 Pilares del SGA.....	123
Figura N° 32 Herramientas de control de MA	123
Figura N° 33 Las 5 fuerzas de Porter.....	128
Figura N° 34 Formato de registro de asistencia	128
Figura N° 35 Matriz IPERC.Anverso	135
Figura N° 36 Matriz IPERC.Reverso	136
Figura N° 37 Entrevista desarrollada	138
Figura N° 38 Inventario de Hardware.....	139
Figura N° 39 Inventario de Software	140
Figura N° 40 Formato de restauración de información.....	141
Figura N° 41 Filtrado MAC	142
Figura N° 42 Intervalo de confiabilidad de Cronbach.....	156
Figura N° 43 Participación en el uso de herramientas de SI.....	157
Figura N° 44 Participación En La Seguridad De Los Sistemas.....	158
Figura N° 45 Participación en la identificación del riesgo en TI	159
Figura N° 46 Participación en proyectos tecnológicos	160

Figura N° 47 Participación en ejecución de pruebas de control.....	161
Figura N° 48 Intervalo de confiabilidad de Cronbach.....	165
Figura N° 49 Control al sistema de información.....	166
Figura N° 50 Control de recursos de infraestructura tecnológica.....	167
Figura N° 51 Control de recursos de software.....	168
Figura N° 52 Metodología de implementación.....	169
Figura N° 53 Estrategia del sistema de información.....	170
Figura N° 54 Intervalo de confiabilidad de Cronbach.....	174
Figura N° 55 Control al sistema de información.....	175
Figura N° 56 Segregación de funciones en el sistema de información.....	176
Figura N° 57 Políticas de seguridad y acceso al sistema.....	177
Figura N° 58 Diagrama de dispersión de correlación.....	180
Figura N° 59 Diagrama de dispersión de correlación.....	182

RESUMEN

La investigación desarrollada tiene como objetivo demostrar el grado de mejora del desempeño de mecanismos de seguridad de la información alineados a normas, buenas prácticas y estándares internacionales aplicados en la gestión de Seguridad de la Información.

¿Cuál es el estado de la gestión de seguridad de la información en la industria minera? ¿Los usuarios conocen herramientas de seguridad? ¿Los responsables están conscientes de los riesgos de seguridad?

Luego de establecer el planteamiento del problema se definen los objetivos, para ver la relación entre el desempeño de la seguridad - usuarios – empresa.

Después se definió el marco teórico, se recurrió a normas internacionales con el fin de conocer las mejores prácticas, lineamientos, conceptos, herramientas en la gestión de seguridad de la información.

Una vez definidas las herramientas y diseño del experimento, se encuestó a los integrantes de la muestra para la investigación. Se totalizaron los datos recopilados, la interpretación de estos resultados resultó ligeramente preocupante.

A continuación, se implementaron los planes de acción, herramientas, procedimientos recopilados que más se alineaban a solucionar los problemas analizados.

Para continuar con una segunda recopilación de datos, de la cual quedo demostrando que la participación del usuario tiene una directa relación con el desempeño de los mecanismos de seguridad de la información. Así como la

planificación de los sistemas de información tiene una directa relación con el desempeño de los mecanismos de seguridad de la información.

Finalmente, en conclusiones establecemos lo importante de la investigación para conocer el estado actual, y desarrollar alternativas de solución. En sugerencias se transmite la necesidad de una mayor conciencia de la seguridad de la información y se hace una invitación a investigadores del rubro llegar a implementar un Sistema de Gestión de Seguridad de la Información.

INTRODUCCIÓN

La diferenciación, la globalización, la competencia, la economía, las regulaciones del estado, demandan que las empresas del Perú y del mundo incorporen tecnologías de la información para apoyar sus procesos, esto es más un factor necesario que opcional. Los sistemas de información son cruciales para aprovechar las oportunidades ofrecidas por la globalización generando un alto grado de dependencia de la empresa a estos sistemas.

La información es considerada como el activo fijo con más valor en las empresas, el sector minería no es la excepción, sin embargo, muchas veces no se ve así, la información generada puede ser determinante para permanecer la empresa.

Las empresas continuamente generan información que necesitan usar para la toma de decisiones, dicha información debe ser confidencial, íntegra y disponible, sin embargo, el crecimiento continuo de esta información, así como la cantidad de equipos usados para almacenarla está causando problemas en su correcta gestión.

En estos días la seguridad de la información es mucho más que herramientas de protección de la información; ya que, sin lineamientos, planes de acción o conceptos implantados en la organización, estas herramientas serán de poca ayuda.

Es por ello que recurrimos a normas internacionales ISO, estándares internacionales como ITIL y COBIT para tener un correcto concepto de gestión de la seguridad de la información y su criticidad para garantizar la continuidad

de la empresa.

La presente investigación busca reflejar la situación de la gestión de la seguridad informática en una de las industrias más grandes del país como lo es la minería, evaluando el desempeño y grado de mejora de mecanismos de control de seguridad de la información implementados.

El Capítulo I, se definen los antecedentes del estudio, donde se detalla la problemática de la seguridad de la información en la empresa, la identificación y definición de variables, así como los objetivos y supuestos de la investigación.

El Capítulo II, se revisa el marco teórico, donde se plasma todo el parafraseo de las variables, producto de la bibliografía revisada.

El Capítulo III, presenta el Marco Referencial, que define la descripción de la empresa Minsur y la unidad minera Pucamarca.

El Capítulo IV, desarrolla el marco metodológico en el cual se procede a explicar el desarrollo de la investigación, el procesamiento de los datos obtenidos, así como sus resultados.

CAPÍTULO I

ANTECEDENTES DE ESTUDIO

En el presente capítulo, se brinda un alcance general acerca del presente estudio, paso esencial para determinar el problema, objetivo e hipótesis; conjuntamente de definir la variable dependiente e independiente; de la misma manera la metodología de la investigación, los alcances y limitaciones de la misma.

1.1 TÍTULO DEL TEMA

“Estudio del desempeño de mecanismos de seguridad de la información en empresas mineras, Tacna 2019”

1.2 PLANTEAMIENTO DEL PROBLEMA

La unidad minera Pucamarca Minsur, perteneciente al grupo Breca posee un área de Tecnologías de la Información y Comunicaciones la cual se encarga de abstraer los múltiples roles de las TIC en la unidad minera, siendo uno de estos la gestión de la seguridad de la información.

Vanegas Devia y Pardo (2014) comentaban que en empezando el año 2000, las fábricas de software no utilizaban un sistema metodológico para gestionar el riesgo en sus respectivos proyectos, sino que se enfocaban en lograr un desarrollo que diera respuesta al problema en el que se encontraban trabajando, haciendo una analogía con la realidad peruana actual, este escenario es común en muchas empresas como en la que se realizó la investigación, existe una falta de concientización acerca de los riesgos de seguridad de la información y sus consecuencias a los cuales están expuestos.

La gestión de la seguridad de la información es una labor difícil, más que desde un punto de vista técnico es complejo desde un punto de vista organizacional por ende es necesario implementar estrategias de gestión de seguridad de la información que contengan desarrollo, revisión y cumplimiento de políticas, con solo pensar que un trabajador abandone la empresa, elimine información, suplante identidades o robe información clasificada implicaría un abanico de posibles problemas organizativos,

Una vez más Vanegas Devia y Pardo (2014) comentan que se puede disminuir la pérdida de dinero en los proyectos, si es que se identifican riesgos y se elabora un plan para mitigarlos.

Finalmente es crítico evaluar la mejora de la gestión de la seguridad de la información, teniendo marcos de referencia internacionales de alto grado de aceptación como ISO, ITIL, COBIT que proponen modelos de madurez sólidos en este tema.

1.3 FORMULACIÓN DEL PROBLEMA

1.3.1 PROBLEMA GENERAL

- a. Últimamente se han desencadenado problemas de seguridad de la Información de la empresa, ¿será posible mejorar el desempeño de los mecanismos de seguridad de la información?

1.3.2 PROBLEMAS ESPECÍFICOS

- b. ¿Si mejoramos la participación del usuario en la implementación de sistemas de información mejorará el desempeño de la seguridad de la información de la empresa?
- c. ¿Si mejoramos la planificación de los sistemas de información mejorará el desempeño de seguridad de la información de la empresa?

1.4 HIPÓTESIS

1.4.1 HIPÓTESIS GENERAL

- a. Existe un mejor desempeño de los mecanismos de seguridad de la información en la empresa luego de analizar y mejorar la relación con sus variables más importantes

1.4.2 HIPÓTESIS ESPECÍFICAS

- b. La participación del usuario influye en el desempeño de los mecanismos de seguridad de la información en la empresa.

- c. Existe una relación entre la planificación de los sistemas de información y el desempeño de los mecanismos de seguridad de información en la empresa.

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

- a. Establecer un grado de mejora del desempeño de los mecanismos de seguridad de la información en la empresa.

1.5.2 OBJETIVOS ESPECÍFICOS

- b. Comprobar la influencia de la participación del usuario en el desempeño de los mecanismos de seguridad de la información de la empresa.

- c. Comprobar la relación de la planificación de los sistemas de información en el desempeño de los mecanismos de seguridad de la información de la empresa.

1.6 JUSTIFICACIÓN

La seguridad de la información tiene como objetivo el desarrollo y uso de mecanismos, procedimientos y buenas prácticas para proteger la información de la empresa, dicha información es considerado uno de los activos más importantes para cualquier organización.

Estar al tanto e implementar este tipo de controles, haciendo uso de metodologías establecidas con alto grado de aceptación a nivel global como Cobit, Coso e Itil es necesario; considerando el grado de madurez de empresas del rubro minero.

Además, con el desarrollo y uso adecuado de estas buenas prácticas y mecanismos de seguridad de la información, la empresa contará con políticas, medidas de control y planes de acción que mitigaran la probabilidad de desarrollar riesgos de seguridad de la información.

1.7 METODOLOGÍA

Se realizó un estudio que implica desarrollar dos variables dependientes con una variable independiente en el mismo lapso de tiempo.

La metodología seleccionada en este trabajo será de tipo correlacional dado que se midió el nivel de relación que existe entre dichas variables en un tiempo determinado, se cuantificaron las variables aparentemente relacionadas y estudiará la correlación existente. El diseño de la investigación será experimental, transversal – correlacional.

El instrumento se aplicará a los trabajadores de la unidad minera Pucamarca Minsur, durante el periodo de mayo del 2018 hasta abril del 2019. Se hizo uso de instrumentos como la encuesta, cuestionario estructurado, entrevista y ficha de datos, estos serán cuantificados a través de un modelo de encuesta definida por el método de evaluaciones en la escala de Likert.

1.8 DEFINICIONES

En esta sección se definirá operacionalmente las variables seleccionadas para la investigación.

Variable independiente: Desempeño de mecanismos de seguridad de la información

Para definir mejor esta variable vamos a desglosar el término en dos partes:

Primero, el desempeño es la consecuencia de medir el rendimiento de un determinado fenómeno acción.

Segundo, los mecanismos de seguridad de la información son el conjunto de herramientas de software, gestión y control usados en la empresa para resguardar la seguridad de la información privada.

Uniéndolos ambos términos podemos definir esta variable como el resultado de medir el rendimiento de los mecanismos de seguridad de la información en un determinado lapso de tiempo.

Tabla 1
Operacionalización de la variable independiente

VARIABLE	INDICADORES	ITEMS	ESCALA	RANGOS
Desempeño de mecanismos de seguridad de la información	Control y procedimientos de acceso al SI	1	1=Totalmente en desacuerdo	DEFICIENTE 3-7 REGULAR 8-11 EFICIENTE 12-15
	Segregación de funciones en el SI	2	2=En desacuerdo 3=Ni de acuerdo ni en desacuerdo	
	Políticas de seguridad y acceso al sistema	3	4=De acuerdo 5=Totalmente de acuerdo	

Nota: Elaboración propia

Variable dependiente: Participación del usuario

Podemos definir esta variable como el grado de intervención del usuario en los procesos que comprenda la variable independiente 'desempeño de mecanismos de seguridad de la información', dado que los usuarios son los principales actores en el uso de los sistemas de información. Esta variable conceptualiza el involucramiento e interacción de los usuarios con los sistemas de información de la empresa.

Tabla 2
Operacionalización de la variable dependiente PU

VARIABLE	INDICADORES	ITEMS	ESCALA	RANGOS
Participación del usuario	Participación en el uso de herramientas de seguridad de la información de su empresa	1		
	Participación en la seguridad de los SI	2	1=Totalmente en desacuerdo	
	Participación en la identificación del riesgo en TI	3	2=En desacuerdo	DEFICIENTE 5-11
	Participación en proyectos tecnológicos	4	3=Ni de acuerdo ni en desacuerdo	REGULAR 12-18
	Participación en la ejecución de pruebas de control	5	4=De acuerdo	EFICIENTE 19-25
			5=Totalmente de acuerdo	

Nota: Elaboración propia

Variable dependiente: Planificación de los sistemas de información

Podemos definir esta variable como el grado de participación de la empresa en los procesos que comprenda la variable independiente 'desempeño de mecanismos de seguridad de la información' desde un punto de vista más holístico, dado que la empresa realiza la planificación de los sistemas de

información a implementarse, es crítico medir su involucramiento en la relación entre procesos y sistemas de información. Esta variable conceptualiza el grado de planificación de los sistemas de información en actualización e implementación dentro de un periodo de tiempo.

Tabla 3
Operacionalización de la variable dependiente PS

VARIABLE	INDICADORES	ITEMS	ESCALA	RANGOS
Planificación de los Sistemas de Información (PS)	Control al SI	1		
	Control de recursos de infraestructura tecnológica	2	1=Totalmente en desacuerdo 2=En desacuerdo	DEFICIENTE 5-11 REGULAR 12-18 EFICIENTE 19-25
	Control de recursos de software	3	3=Ni de acuerdo ni en desacuerdo	
	Metodología de implementación	4	4=De acuerdo 5=Totalmente de acuerdo	
	Estrategia de SI	5		

Nota: Elaboración propia

1.9 ALCANCES Y LIMITACIONES

El estudio se realizó midiendo el desempeño de los controles de seguridad de la información en relación con la participación del usuario y planificación de los sistemas de información, durante el periodo de los años 2018 - 2019.

Esta investigación se desarrolló en la unidad minera Pucamarca – Minsur, teniendo en particular que las operaciones mineras se encuentran en zonas geográficas de acceso complejo (por lo general) y altos estándares de seguridad patrimonial, complicando la recopilación de información de los usuarios. Del mismo modo estas empresas deberían tener una cultura de TIC desarrollada salvaguardando el nivel de acceso público a estas.

El realizar este estudio implicaría tener acceso a conocer el escenario del área de TIC en la operación minera Pucamarca - Minsur, ubicada en Tacna.

CAPÍTULO II

MARCO TEÓRICO

2.1 CONCEPTUALIZACIÓN DEL DESEMPEÑO DE MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

Conceptualizaremos la variable “desempeño de mecanismo de seguridad de la información” como el acto de aplicar mecanismos de seguridad de la información en un escenario y medir sus consecuencias.

2.1.1 MECANISMOS DE SEGURIDAD SEGÚN X800

Según Stallings (2004) vemos la tabla 4 y 5 que muestra los mecanismos de seguridad determinados en el estándar X.800. Algunos mecanismos se implementan en una capa específica de un protocolo y algunos que no son específicos de ninguna capa de protocolo o servicio de seguridad en particular. El estándar X.800 diferencia entre mecanismos de cifrado reversible y los mecanismos de cifrado irreversible. El primero se define como un algoritmo de cifrado que permite cifrar los datos y posteriormente, descifrarlos. Y el segundo, los mecanismos de cifrado irreversible incluyen algoritmos hash y códigos de autenticación de mensajes empleados en firmas digitales y en aplicaciones de autenticación de mensajes. En la tabla 6 basada en X.800, podemos apreciar la relación que se da entre los servicios de seguridad y los mecanismos de seguridad

Tabla 4

Mecanismos específicos de seguridad definidos en el estándar X.800

MECANISMOS ESPECIFICOS DE SEGURIDAD
Posibles de ser incorporados en la capa de protocolo adecuada para proporcionar algunos de los servicios de seguridad OSI.
Cifrado
Aplicación de algoritmos matemáticos para transformar datos de una forma inteligible. La conversión y la posterior recuperación de los datos depende de un algoritmo y cero o más claves de cifrado.
Firma digital
Datos añadidos a, o una transformación criptográfica de, una unidad de datos que da la capacidad al receptor verificar la fuente y la integridad de la unidad de datos y protegerla de la falsificación (por parte del receptor).
Control de acceso
Una serie de mecanismos que fortalecen los derechos de acceso a los recursos.
Integridad de los datos
Una serie de mecanismos empleados para validar la integridad de una unidad de datos o del flujo de unidades de datos.
Intercambio de autenticación
Un mecanismo diseñado para validar la identidad de una entidad por medio del intercambio de información.
Relleno del trafico
La inserción de bits en espacios de un flujo de datos para mitigar los intentos de análisis de tráfico.
Control de enrutamiento
Permite la selección de rutas físicamente seguras para determinados escenarios y permite los cambios de enrutamiento, especialmente cuando se sospecha de una brecha en la seguridad.
Notarización
El uso de una tercera parte confiable para asegurar algunas propiedades en un intercambio de datos.

Nota: Adaptado de Fundamentos de seguridad en redes, Stallings (2004).

Tabla 5

Mecanismos generales de seguridad definidos en el estándar X.800

MECANISMOS GENERALES DE SEGURIDAD

Mecanismos que no son puntuales de ninguna capa de protocolo o sistema de seguridad OSI en particular.

Funcionalidad fiable

La que se considera correcta con respecto a algunos factores (por ejemplo, los establecimientos por una política de seguridad).

Etiquetas de seguridad

La marca asociada a un recurso (que podría ser una unidad de datos) que establece los atributos de seguridad de ese recurso.

Detección de acciones

Detección de acciones vinculadas con la seguridad.

Informe para la auditoría de seguridad

Recopilación de datos para facilitar una auditoría de seguridad, que consiste en una revisión y un examen independiente de los informes y actividades del sistema.

Recuperación de la seguridad

Maneja las solicitudes de los mecanismos (como funciones de gestión de acciones) y lleva a cabo acciones de recuperación.

Nota: Adaptado de Fundamentos de seguridad en redes, Stallings (2004).

La figura 1 compone un modelo que muestra en términos generales, gran parte de los aspectos que discutiremos. La idea es que un mensaje sea transmitido de una parte a otra parte mediante algún tipo de internet. Las dos partes (interlocutores) en esta transacción, han de cooperar para que el intercambio tenga lugar. Se define un solo canal de información por una ruta a través de la internet, para que vaya desde el emisor al receptor y a través el uso

cooperativo de los protocolos de comunicación (TCP/IP) por parte de ambos participantes.

Tabla 6
Relación entre servicios de seguridad y ataques

Ataque						
Servicio	Obtención del contenido del mensaje	Análisis de tráfico	Suplantación	Repetición	Modificación de mensajes	Interrupción de servicios
Autenticación de entidades origen/ destino			X			
Autenticación del origen de los datos			X			
Control de acceso			X			
Confidencialidad	X					
Confidencialidad del flujo del tráfico		X				
Integridad de los datos				X	X	
No repudio						
Disponibilidad						X

Nota: Adaptado de Fundamentos de seguridad en redes, Stallings (2004)

Los aspectos de seguridad se ponen en juego cuando es necesario o se quiere proteger la transmisión de la información de un oponente que pudiera representar una amenaza a la confidencialidad, a la autenticidad, etc. Todas las técnicas para brindar seguridad suelen tener dos componentes:

- Una transformación vinculada con la seguridad de la información que se

enviará. Por ejemplo, tenemos el cifrado del mensaje el cual provoca que resulte ilegible debido al cambio de palabras, además de la aplicación de un código basado en el contenido del mensaje, que puede usarse para identificar al emisor.

- Cierta información secreta conocida entre los interlocutores y desconocida por el oponente. Por ejemplo, una clave de cifrado en conjunto con la transformación para desordenar la información del mensaje antes de la transmisión y reordenarlo en el momento de la recepción.

Tabla 7
Relación entre servicios y mecanismos de seguridad

Servicio	Mecanismo							
	Cifrado	Firma digital	Control de acceso	Integridad de los datos	Intercambio de Autenticación	Relleno del tráfico	Control de enrutamiento	Notarización
Autenticación de entidades origen/ destino	X	X			X			
Autenticación del origen de los datos	X	X						
Control de acceso			X					
Confidencialidad	X						X	
Confidencialidad del flujo del tráfico	X					X	X	
Integridad de los datos	X	X		X				
No repudio		X		X				X
Disponibilidad				X	X			

Nota: Adaptado de Fundamentos de seguridad en redes, Stallings (2004).

Con el fin de lograr una transmisión aún más segura, existe la posibilidad de que sea necesaria una tercera parte confiable, que sea la garante de distribuir la información privada a los dos interlocutores y la proteja de cualquier oponente. Es posible que también sea necesaria para arbitrar disputas entre los dos interlocutores en lo relativo a la autenticidad de la transmisión de un mensaje.

En el presente modelo general podemos ver que existen cuatro tareas básicas en el diseño de un servicio de seguridad de la información:

1. Elaborar un algoritmo que llevará a cabo la transformación relacionada con la seguridad. El algoritmo estará diseñado para que ningún oponente pueda interrumpir el mensaje.
2. Producir los datos privados que serán usados para el algoritmo.
3. Desarrollar métodos con la finalidad de distribuir y compartir la información secreta.
4. Definir un protocolo para los dos interlocutores, haciendo uso del algoritmo de seguridad y la información secreta, con la finalidad de obtener un servicio sólido de seguridad.

La segunda parte del libro citado, conceptualiza los tipos de mecanismos y servicios de seguridad que se adaptan al modelo que muestra la figura 1. Sin embargo, existen otros escenarios relacionados con la seguridad que son de

interés y que no se corresponden claramente con este modelo, pero que también se han de considerar. La figura 2 muestra un modelo general de estos escenarios, que manifiesta la necesidad de proteger un sistema de información al acceso no deseado. La gran mayoría de usuarios están familiarizados con los problemas causados por las acciones de los hackers, que tratan de vulnerar sistemas a los que se puede acceder por una red. El atacante no necesariamente tiene el objetivo de provocar daño, pero si consigue satisfacerse por el simple hecho de romper y vulnerar la seguridad en sistemas informáticos. El hacker también podría ser personal de la empresa contrariado, que quiere hacer daño, o un delincuente que intenta explotar los sistemas computacionales con la finalidad de conseguir beneficios financieros (obtención de códigos de tarjetas de crédito o transferencias ilícitas de dinero a otras cuentas).

Otro ejemplo de acceso no deseado podría ser el de infiltrar en un sistema de información alguna aplicación que explote vulnerabilidades del sistema y que pueda dañar a los programas de aplicaciones y sistemas de información.

Existen dos tipos de amenazas para estos programas:

- Amenazas al acceso a la información: Modificación de la información realizada por usuarios que no deberían poder acceder a dichos datos.
- Amenazas al servicio: Aprovechar errores en el sistema en los ordenadores para imposibilitar su uso por parte de los usuarios.

Dos ejemplos de ataques mediante software serían los virus y gusanos. Dichos ataques podrían infiltrarse en un sistema a través de una unidad usb que almacene algún software no deseado oculto. Asimismo, es posible que sean infiltrados al sistema a través de una red; sin embargo, esta modalidad es parte de interés en la seguridad de redes.

Los mecanismos de seguridad precisos para afrontar a accesos no deseados son divididos en dos segmentos como se ve en la figura 2. El primer segmento es el que funciona acorde a la vigilancia, el cual incluye los procedimientos de conexiones a través de contraseñas los cuales fueron elaborados para bloquear el acceso a usuarios sin permiso y los softwares de ocultación, elaborados para identificar y eliminar gusanos, virus y ataques similares.

El segundo segmento establece la línea de defensa como una serie de controles internos que monitorean los procesos y analizan la información guardada con la finalidad de detectar la presencia de intrusos.

Figura 1

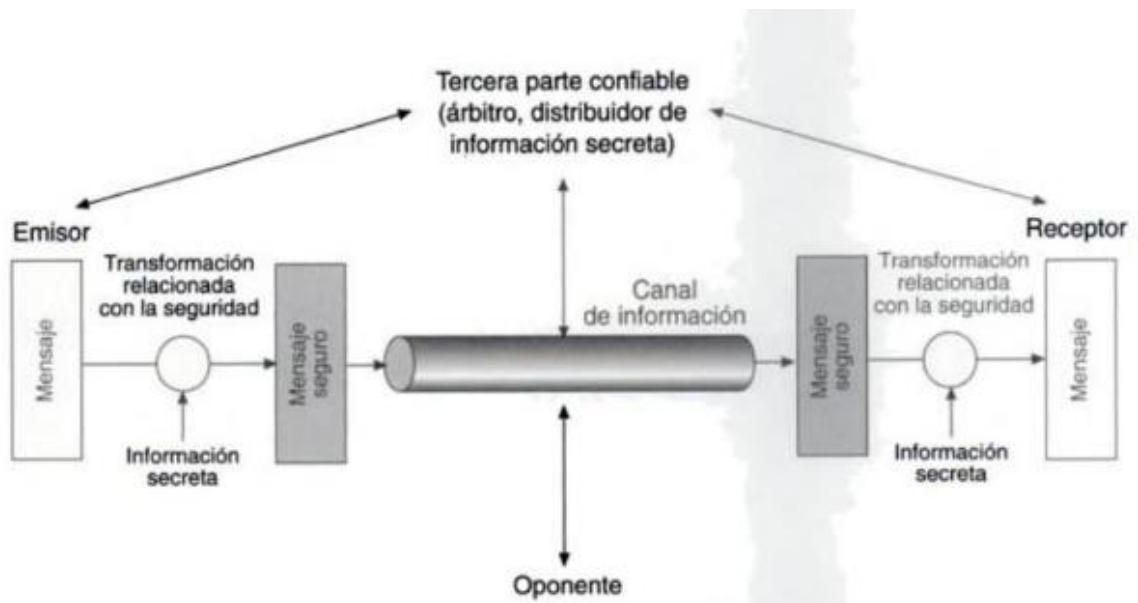


Figura 1. Modelo para la seguridad de redes. Reimpreso de Comunicaciones y redes de computadores. Copyright 2001 por William Stallings.

Figura 2



Figura 2. Modelo para la seguridad en el acceso a redes. Reimpreso de Fundamentos de seguridad en redes. Copyright por William Stallings (2004)

2.1.2 COBIT

Según Control Objectives for Information and related Technology [COBIT] (2007) en su versión 4.1, la necesidad de conservar la integridad de la información y de salvaguardar los activos de TI, demanda de un proceso de administración de la seguridad de la información. Dicho proceso incluye la definición y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de IT. Administrar la seguridad de la información también implica realizar correcciones acerca de las vulnerabilidades o eventos de seguridad identificados, de la misma forma realizar monitoreos de seguridad y pruebas programadas. Realizar bien la administración de la seguridad salvaguarda todos los activos de TI minimizando el impacto en el negocio a causa de posibles vulnerabilidades o eventos de seguridad.

Controlar los procesos TI con el objetivo de

- Garantizar la seguridad de los sistemas de información

Que satisface el requerimiento del negocio de TI para

- Conservar la integridad de la información y de la infraestructura de procesamiento además de mermar el impacto de las vulnerabilidades e eventos de seguridad.

Haciendo enfoque en

- La introducción de políticas, buenas prácticas y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e eventos de seguridad.

Se logra a través de

- Comprender los requisitos, vulnerabilidades y amenazas de seguridad.
- La gestión estandarizada de identidades y autorizaciones de los usuarios.
- Probando la seguridad de forma periódica.

Y es posible cuantificarlo a través de

- La cantidad de incidentes que afectan la reputación con el público.
- La cantidad de sistemas que no cumplen los requerimientos de seguridad.
- La cantidad de violaciones en la segregación de tareas.

Figura 3



Figura 3. Pentágono de Gobierno de TI. Reimpreso de COBIT 4.1. Copyright 2001 por Institute IT Governance

2.1.3 ITIL

Según Information Technology Infrastructure [ITIL] (2008) en su versión 3, el sistema de Gestión de la Seguridad de la Información (ISMS), brinda las bases para el eficiente progreso de un programa de seguridad de la información que beneficie los objetivos del negocio. Con el fin de garantizar que se han determinado altos niveles de seguridad, utilizaremos la metodología de las 4 “P” de: Personas, Procesos, Productos (incluyendo tecnología) y Partners (incluyendo suministradores de servicios).

La ISO 27001 es el estándar internacional con la que las instituciones tendrán la posibilidad de diferenciar y certificar su ISMS. La Figura 4 está apoyada en distintas buenas prácticas (incluyendo ISO 27001) y presenta los cinco elementos y sus objetivos

Figura 4



Figura 4.

Figura 4. Marco para la gestión de seguridad de TI. Reimpreso de ITIL. Copyright 2008 por Van Haren Publishing

Gobierno de la seguridad

Un gobierno de seguridad de TI permite proporcionar seis resultados:

- Alineación estratégica:
 - Los requerimientos de seguridad deberían originarse según los requisitos empresariales.
 - Las soluciones de seguridad deberán concordar con procesos de la empresa.
- Creación de valor:
 - Grupo estandarizado de prácticas de seguridad.
 - Desempeño especial y equitativo sobre aquellas áreas de mayor importancia en el rendimiento del negocio.
- Gestión del riesgo:
 - Perfiles de riesgo.
 - Importancia de la gestión del riesgo
- Gestión del rendimiento:
 - Indicadores bien definidos, establecidos y funcionando.
 - Establecer las acciones que ayuden a buscar vulnerabilidades.
- Gestión de recursos:
 - Documentar y tener siempre disponibles la información.
 - Documentar los procesos de seguridad.
- Asegurarse procesos de negocio.

El encargado de gestionar la seguridad de la información debe tener conocimiento de que la seguridad no es sólo un paso más en el Ciclo de Vida y que no puede ser garantizada solo por la tecnología. La seguridad de la información es periódica, un proceso continuo que necesita una gestión, y debe ser una parte integral de todos los servicios (y sistemas). La Figura 5

describe los controles que se suelen usar en el proceso.

Figura 5

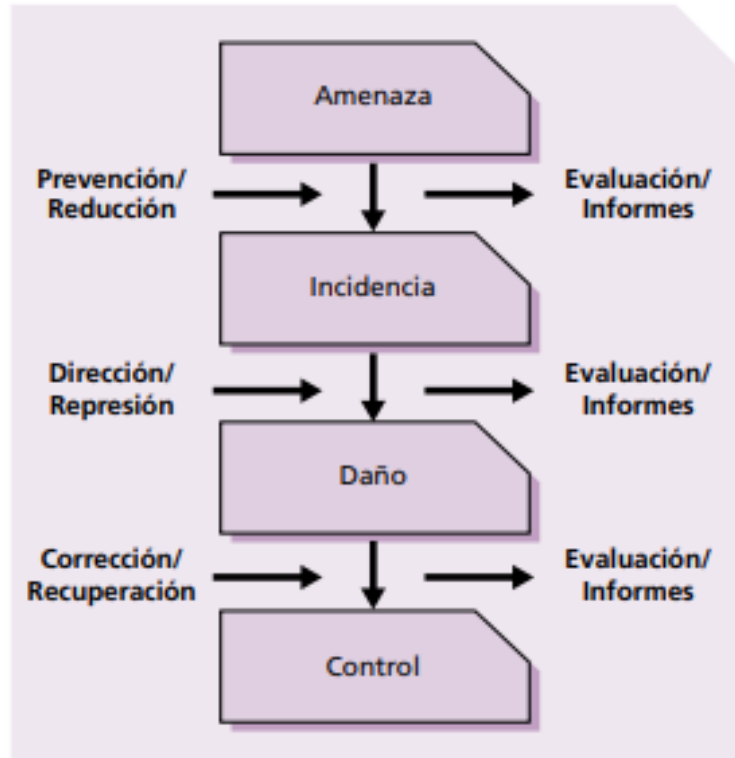


Figura 5. Controles de seguridad para amenazas e incidencias. Reimpreso de ITIL. Copyright 2008 por Van Haren Publishing

La figura indica que un riesgo puede llegar a convertirse en una amenaza que, a su vez, provocaría una incidencia que produce daños. Sin embargo, a lo largo de estas fases se pueden tomar medidas de distinta naturaleza:

- Medidas preventivas para prevenir efectos (ejemplo, gestión de accesos).
- Medidas reductivas para limitar efectos (ejemplo, backup y pruebas).
- Medidas indagadoras para detectar efectos (ejemplo, monitorización).
- Medidas represivas para suprimir efectos (ejemplo, bloqueo).

- Medidas correctivas para reparar efectos (ejemplo, retirada).

Gestión de la información

Los datos imprescindibles donde se aplicará la gestión de la seguridad de la información, se deben almacenar en un sistema ISMS que contemple factores sobre controles de seguridad, riesgos, fallos, procesos e informes.

El ISMS deberá velar por todos los servicios de TI de la empresa y debe estar integrada en otros sistemas de gestión de TI, especialmente en la Cartera de Servicios y el Sistema de Gestión de la Configuración.

El Sistema de Gestión de la Seguridad de la Información y la política de seguridad de la información deben ser asistidas por el soporte y el mantenimiento necesarios.

2.1.4 AMENAZAS DE SEGURIDAD

Según Stallings (2001) comenta que para poder comprender las amenazas a la seguridad que existen y sus distintos tipos, debemos establecer los requisitos en seguridad. La seguridad en ordenadores y en redes se basa en tres requisitos básicos:

- **Secreta:** Establece que la información sea de acceso de edición o lectura sólo por personal autorizados. Esta comprendido en este tipo de permisos imprimir, visualizar en pantalla y demás formas de revelación que incluye cualquier manera de revelar la existencia de un objeto.
- **Integridad:** Establece que la información sea modificada solamente por personal autorizado. La modificación incluye escribir, cambiar, cambiar de estado, suprimir y crear.
- **Disponibilidad:** requiere que la información esté disponible solo a personal autorizado.

En la figura 6 podemos ver una clasificación de las agresiones a la seguridad en red que se hace en términos de agresiones pasivas y agresiones activas.

Ataques pasivos

Los ataques pasivos son del tipo de monitorizaciones. de las transmisiones. La finalidad del hacker es conseguir datos que estén siendo transmitidos. Tenemos dos tipos de ataques: divulgación del contenido de un mensaje y análisis del tráfico.

La divulgación del contenido de un mensaje se puede sobre entender como difundir una conversación por audio, un mensaje de texto o un archivo

transferido que puede contener información sensible o privados. Así, sería deseable prevenir que el hacker se entere del contenido de estas transmisiones.

La segunda manera de agresión pasiva es el análisis del tráfico, es más sutil. Suponga que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, a pesar de que se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más usada para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría averiguar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Con esta información podría extraer la naturaleza de la comunicación que se está realizando.

Los ataques pasivos son más complicados de detectar ya que no implican la alteración de los datos. No obstante, es factible prevenir el éxito de estas agresiones. Así, el objetivo para tratar estas agresiones está en la prevención antes que la detección.

Figura 6

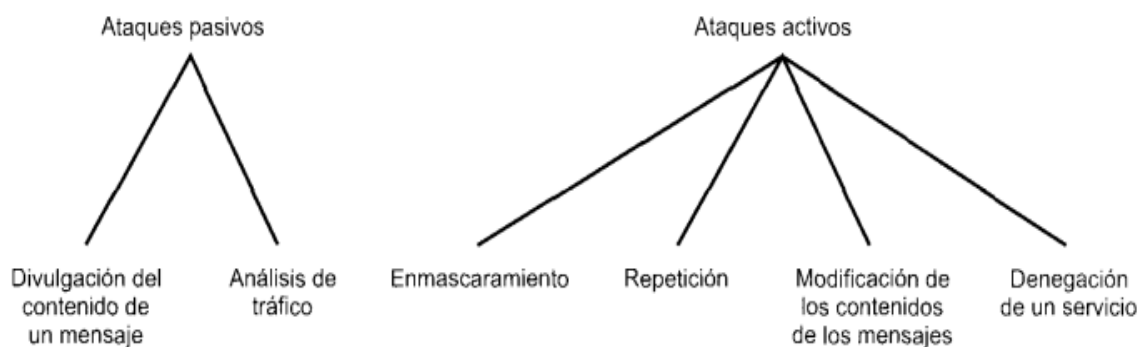


Figura 6. Agresiones a la seguridad de red activas y pasivas. Reimpreso de *Comunicaciones y redes de computadores*. Copyright 2001 por William Stallings.

Ataques activos

Son definidos como todo cambio del flujo de datos o la generación de flujos falsos, son divididos en 4 tipos: enmascaramiento, repetición, modificación de mensajes y denegación de servicio.

Enmascaramiento: Se desarrolla cuando un objeto aparenta ser otro y normalmente incluye alguna de las otras formas de agresión activa. Por ejemplo, si es que se obtiene una secuencia de autenticación y se permuta por otra secuencia de autenticación válida, así se da la posibilidad a otra entidad autorizada permisos limitados a ganar otros permisos, suplantando a la entidad que los tiene.

La repetición define secuestrar pasivamente unidades de datos, volver a enviarlas repetitivamente y subsecuente con el objetivo de generar un resultado no autorizado.

La modificación de mensajes implica alguna alteración de parte del mensaje, o un retraso inesperado del mismo, también algún cambio en su orden para producir consecuencias inesperadas. Por ejemplo, tenemos un mensaje con que dice «Permitir a Iván Álvarez la lectura del archivo privado de cuentas especiales» se modifica para tener el significado «Permitir a Iván Alvarado la lectura del archivo privado de cuentas especiales».

La denegación de un servicio implica la prevención del uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener como objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes

dirigidos a un destino en específico (por ejemplo, al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la perturbación sobre una red entera, deshabilitándola o sobre cargándola con mensajes de forma que se su rendimiento caiga a tal punto de ser inutilizable.

Las agresiones activas tienen peculiaridades contrarias a las pasivas. Cuando una agresión pasiva es complicada de descubrir, existen distintos métodos de prevención para ella. No obstante, es complicado prevenir una agresión activa, ya que para hacerlo se requeriría protección física constante de todas las rutas y todos los recursos de comunicación. Por ende, el objetivo es identificarlas y recuperarse de cualquier alteración o retardo causados por ellas. Dado que la detección produce una situación disuasiva, podría prevenir de la misma manera.

2.1.5 SERVICIOS DE SEGURIDAD

Según Aguilera Lopez (2004) existen distintos servicios de seguridad como:

- Autenticación (o identificación): Implica que el sistema sea capaz de verificar que un usuario identificado que ingresa a un sistema o que genera una información es quien dice ser. Solo cuando un usuario o entidad ha sido autenticado logrará tener autorización de acceso.
- Disponibilidad: Implica que la información esté disponible en todo momento, cuando sea requerida por las entidades autorizadas.
- Integridad: Implica que los datos del sistema no han sido alterados ni cancelados por personal no autorizado y que el contenido de estos mensajes recibidos es el correcto.
- Control de acceso: Implica poder acceder a los recursos del sistema solamente el personal y usuarios con autorización.
- No repudio (o irrenunciabilidad): Implica proporcionar al sistema una serie de evidencias incuestionables de la autoría de un hecho. El no repudio se basa en no poder negar haber emitido una información que si se emitió y en no poder negar su recepción cuando si ha sido recibida.
- Confidencialidad: Implica protección contra la revelación intencional o accidental de la información en una comunicación.

Es por ello que el no repudio puede darse:

- En origen: El emisor no puede refutar el envío, porque el receptor tiene

pruebas certificadas de dicho envío y de la identidad del emisor. Estas pruebas son emitidas por el propio emisor.

- En destino: En este caso es el destinatario quien no podrá refutar haber recibido el envío, dado que el emisor tiene pruebas infalsificables de dicho envío y de la identidad del destinatario. En este caso será el receptor quien creará las pruebas.

Mecanismos de seguridad

Si los clasificamos en base a la función que desempeñen pueden clasificarse en:

- Correctores: Su objetivo es la corrección de los resultados de algún daño. Se desarrollan luego de que se haya suscitado un ataque y haya desencadenado daños.
- Preventivos. Funcionan antes que se efectúe el ataque. Su misión es evitarlo.
- Detectores. Funcionan antes de que se desarrollen daños y cuando el ataque se ha suscitado, monitorean el sistema.

La selección de mecanismos de seguridad será acorde a cada sistema de información, de las posibilidades económicas de la institución, sus funciones y los posibles riesgos a los que este expuesto el sistema.

Existen muchos y distintos mecanismos de seguridad, cada uno ofrece al sistema uno o más servicios de seguridad. Aquí mencionaremos a los más comunes.

Seguridad lógica

Las herramientas de seguridad lógica tienen como misión proteger digitalmente la información de manera directa.

- Control de accesos a través de nombres de usuario y contraseñas
- Cifrado de datos (encriptación). Los datos se infiltrarán con una contraseña específica producto de un algoritmo de encriptación. Solo el emisor y receptor saben cuál es la clave y son ellos los que pueden descifrar el contenido del mensaje.
- Antivirus. Detectan e bloquean la entrada de virus y otro software maliciosos. En el caso de infecciones algunas veces pueden eliminarlos y tienen la característica de reparar los daños ocasionados por algún ataque. Preventivo, detector y corrector, protege la integridad de la información.
- Firma digital. Utilizada para el envío y recepción de mensajes por internet y en la administración de documentos digitales (ejemplo, gestionar bibliotecas digitales). Tiene como finalidad identificar de manera correcta a la persona o al grupo de personas que son responsables del mensaje o del documento. Vela por la integridad y la confidencialidad de la información.
- Certificados digitales. Son archivos digitales a través de los cuales un objeto certificado da la garantía necesaria a una persona o entidad para saber que es quien dice ser, garantizada por la comprobación de su

clave pública. Busca proteger la integridad y la confidencialidad de los datos.

Figura 7



Figura 7. Antivirus, seguridad lógica. Reimpreso de Seguridad informática. Copyright 2004 por Purificación Aguilera.

Figura 8



Figura 8. Firma digital. Reimpreso de Seguridad informática. Copyright 2004 por Purificación Aguilera.

Las redes de tipo inalámbricas (Wifi) por su naturaleza requieren medidas adicionales para su seguridad:

- Usar un SSID (service set identifier), quiere decir establecer una identidad a la red, etiquetarla de preferencia con un nombre que pase desapercibido para terceros con la finalidad de que llamen la atención entre las redes disponibles. Es recomendable renombrar cada cierto tiempo la SSID.

- Protección de la red a través de claves encriptadas WEP (Wired equivalent privacy) o WPA (Wifi protected Access). Una clave WEP implica más recursos y es más fácil de descifrar que una clave WPA y debería cambiarse seguido. La WPA es de encriptación dinámica y más difícil de descifrar por lo cual es más segura. Es recomendable modificar cada cierto tiempo la clave de acceso de red.
- Filtrado de direcciones MAC (media Access control). Es un mecanismo de control de acceso al sistema a través de hardware, por el que se filtran y se permite el acceso solo a algunas direcciones MAC, asumiendo el caso de que toda tarjeta de red debería tener una dirección MAC irrepetible en el mundo. Es posible que resulte complicado de configurar y no es infalible puesto que es posible enmascarar la dirección MAC original.

Seguridad física

Son mecanismos físicos que tienen como objetivo de proteger al sistema (y por tanto indirectamente a la información) de peligros físicos y lógicos.

Figura 9



Figura 9. Detector de humos. Reimpreso de Seguridad informática. Copyright 2004 por Purificación Aguilera.

Figura 10



*Figura 10. SAI (Sistema de alimentación ininterrumpida). Reimpreso de Seguridad informática.
Copyright 2004 por Purificación Aguilera.*

- Respaldo de datos: Creando y guardando copias de seguridad de la información de un determinado sistema en un lugar seguro.
- Dispositivos físicos de protección, por ejemplo, detectores de humo, pararrayos, extintores técnicos, firewall por hardware, sensores contra incendios, sistemas de alimentación eléctrica ininterrumpida (para picos y cortes de corriente eléctrica) o mecanismos de protección contra instalaciones. En cuanto a los usuarios podemos comentar, acceso exclusivo a las ubicaciones; por ejemplo, a través vigilantes jurados o cualquier terminal que excluya la entrada de personas a zonas restringidas.

En esta figura se puede observar visiblemente la interacción entre mecanismos y servicios de seguridad, y de ambos sobre los activos y los peligros a los que están expuestos.

Figura 11

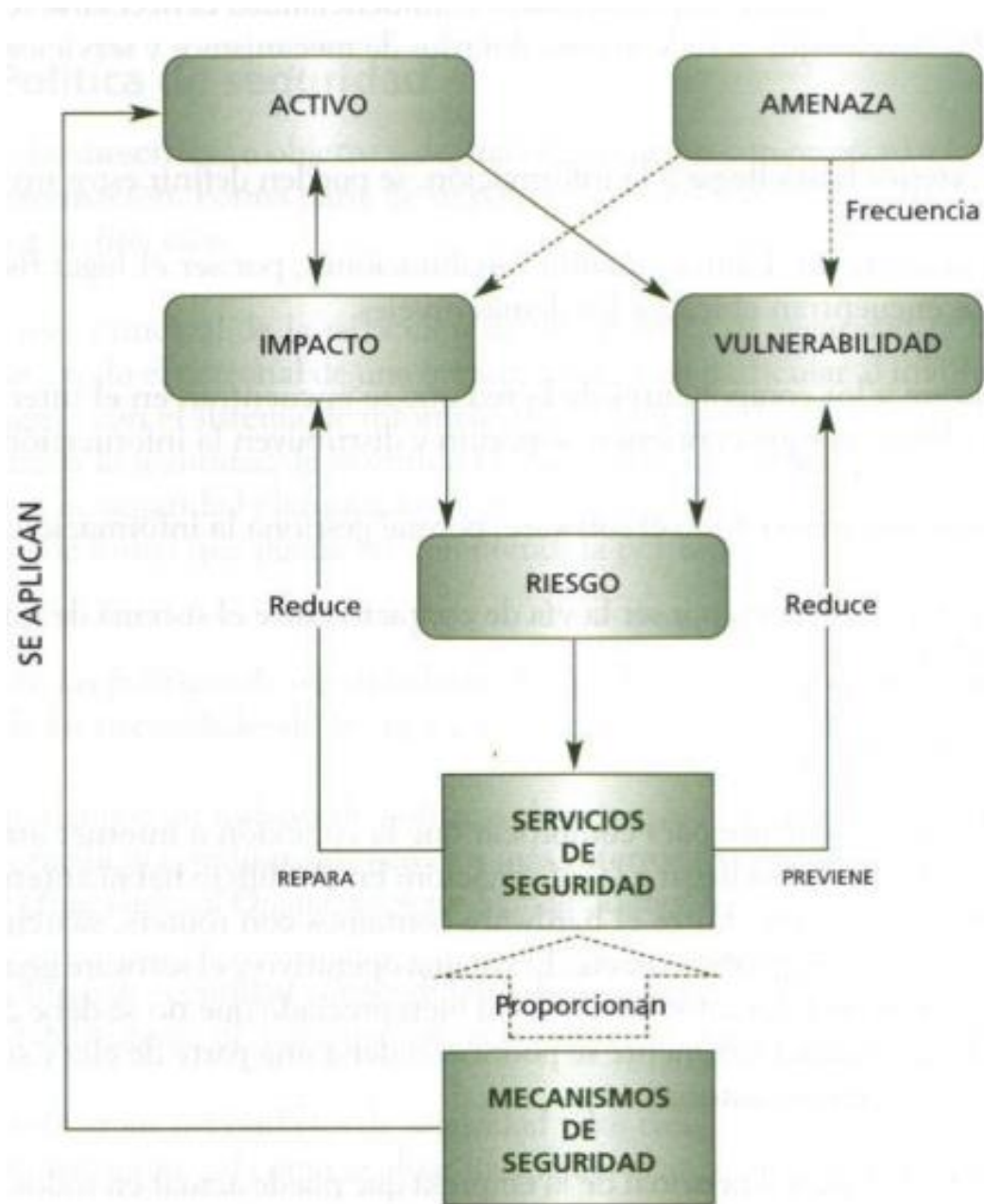


Figura 11. Mecanismos y servicios de seguridad. *Reimpreso de Seguridad informática. Copyright 2004 por Purificación Aguilera.*

2.1.6 CLASES DE MECANISMOS DE SEGURIDAD

Según Areitio Bertolín (2008) los mecanismos de seguridad existen con el objetivo de proporcionar y ofrecer soporte a los servicios de seguridad de la información. Son divididos en dos clases:

1. Mecanismos de seguridad específicos, los cuales proporcionan servicios de seguridad puntuales, tales como integridad, confidencialidad y autenticación. Los cuales son implementados según la arquitectura de comunicación de los siete niveles OSI en un nivel específico.
2. Mecanismos de seguridad generalizados, son no propios de ningún nivel concreto ni servicio de seguridad de OSI. Además, no aplican como específicos para servicios puntuales, por ejemplo, auditoria, responsabilidad, recuperación de seguridad.

Los mecanismos de seguridad específicos

Estos pueden dividirse en ocho tipos:

1. Cifrado de clave pública o asimétrico y de clave privada o simétrico.
2. Firma digital, basada en criptografía de clave pública. Existen sendas modalidades basadas en PKI y en IBC.
3. Mecanismos de control de acceso.
4. Mecanismos de integridad de datos como los MAC, hash o firma digital.
5. Intercambio de autenticación.

6. Relleno de tráfico.
7. Control de encaminamiento.
8. Notarización, con TTP o notarios o fedatarios electrónicos.

Categorías de mecanismos de seguridad generalizados

Entre las categorías de los mecanismos de seguridad generalizados, se han identificado cinco:

1. Funcionalidad de confianza. Hace referencia a que cualquier entidad que proporcione mecanismos de seguridad debe tener confiabilidad. Puede hacerse mediante sistemas que son una combinación de software y hardware.
2. Etiquetas de seguridad. Se encuentran relacionados con el hecho de que, en cualquier recurso, por ejemplo, el almacenamiento de datos, la potencia de procesado o el ancho de banda de un canal de comunicaciones, pueden llevar asociada una etiqueta de seguridad para identificar el grado de sensibilidad de esta. Las etiquetas también pueden vincularse a los datos transferidos y asociarse a los usuarios.
3. Detección de eventos. Incluye la detección de varias acciones: intentos de violación de la seguridad, actividad legítima relativa a la seguridad y, también puede utilizarse para activar informes de eventos y alarmas, hacer un registro de eventos y una recuperación automatizada.
4. Registro de auditoría de seguridad. Tiene como objetivo recabar los eventos pasados relacionados con la seguridad. Permite la detección e

investigación forense de fisuras de seguridad pasadas.

5. Recuperación de la seguridad. Incluye los mecanismos para gestionar solicitudes para recuperarse de los fallos de seguridad. Esto puede incluir la suspensión o cancelación de manera inmediata de las operaciones, la invalidación temporal de una entidad y la inclusión de una entidad en una zona de cuarentena.

Relación ente servicios y mecanismos de seguridad ISO-7498-2 y entre los servicios de seguridad y las capas del modelo OSI

La ISO 7498-2 (1989) comenta que los mecanismos que pueden utilizarse para proporcionar determinados servicios. Realmente, no son unas normas absolutas, ya que tienen ciertas carencias, como la falta de reglamentación en el uso de mecanismo de integridad para ayudar a proporcionar servicios de no repudio como parte de la notarización. El estándar ISO-7498-2 reglamenta la localización de los servicios de seguridad en las diferentes capas del modelo OSI, según se aprecia en la tabla 8.

La norma ISO-7498-2 indica los servicios de seguridad proporcionados para las siete capas. Las capas 1 y 2 proporcionan servicios de confidencialidad solamente. Las capas 3 y 4 proporcionan servicios como la integridad, confidencialidad y autenticación. La capa 7 proporciona todos los servicios. Las capas 5 y 6 proporcionan servicios como la integridad y confidencialidad.

Tabla 8
Servicios de seguridad por nivel OSI según la norma ISO 7496-2

Servicio	CAPA					
	1	2	3	4	5/6	7
Autenticación de entidades			x	X		X
Autenticación del origen			x	X		X
Control de acceso			x	X		X
Confidencialidad con conexión	X	x	x	X		X
Confidencialidad sin conexión		x	x	X		X
Confidencialidad de un campo selectivo						X
Confidencialidad del flujo del tráfico	x		x			X
Integridad con conexión con recuperación				x		X
Integridad con conexión sin recuperación			x	x		X
Integridad con conexión de un campo selectivo						X
Integridad sin conexión			x	x		X
Integridad sin conexión de un campo selectivo						X
No repudio del origen						X
No repudio del destinatario						X

Nota: Adaptado de Seguridad de la información, Bertolín (2008)

Categorías de gestión de la seguridad

El estándar ISO-7498-2 define la gestión de la seguridad como el control y la distribución de información con la finalidad de proporcionar mecanismos y servicios de seguridad, realizar reportes sobre ellos y sobre eventos relacionados con la seguridad. Introduce el concepto de base de información de gestión de seguridad o SMIB (security management information base), que puede incluir tablas de datos y se puede embeber tanto en el software como en el hardware.

Tenemos identificadas cuatro categorías de gestión de seguridad.

1. Gestión de la seguridad del sistema.
2. Gestión del servicio de seguridad.
3. Gestión del mecanismo de seguridad.
4. Seguridad de la gestión OSI.

Gestionar los aspectos de seguridad del sistema de manera completa debería incluir:

- La gestión de las políticas de seguridad.
- La interacción con otras funciones de gestión como la gestión de la contabilidad, la gestión de fallos, la gestión de la configuración y la gestión del rendimiento.
- Gestión de manipulación de eventos.
- Gestión de auditoría de seguridad y recuperación.
- Gestión de la política de control de acceso.

La gestión de claves es fundamental para todo mecanismo, de seguridad, basado en criptografía, y es imprescindible decidir cuándo se necesitan actualizar las claves, generarlas cuando se precisan y distribuirlas de una manera segura. Cuando se diseña un sistema seguro, existen dos consideraciones fundamentales:

- La funcionalidad del sistema.
- El aseguramiento del sistema.

2.1.7 TIPOS DE MECANISMOS DE SEGURIDAD

Según García Cervigón Hurtado y Alegre Ramos (2011) consideran los mecanismos de seguridad como todo aquello de naturaleza de hardware, así como software que utilicemos para crear, reforzar y mantener la seguridad informática.

Dentro de los mecanismos de seguridad podemos distinguir entre:

Mecanismos software o lógicos

Aquí podemos encontrar barreras de software del tipo cortafuegos, antivirus, antispam, manejo de números de serie, protección anticopia, encriptación de los datos, uso de contraseñas, formación a los usuarios del sistema.

Mecanismos de hardware o físicos

Aquí podemos incluir el uso de SAI, extintores, cámaras de seguridad, control de acceso físico al sistema, controles de acceso con tarjetas de proximidad o identificación.

Controlar la temperatura y humedad dentro de una ubicación donde se encuentren los equipos informáticos es otro elemento esencial dentro de los mecanismos de seguridad físicos.

Figura 12



Figura 12. Mecanismos de hardware. Reimpreso de Seguridad informática. Copyright 2001 por García Cervigón Hurtado & Alegre Ramos

Una temperatura demasiado baja o elevada, o un nivel de humedad demasiado alto pueden causar que los equipos no funcionen adecuadamente o incluso producir que estos lleguen a no funcionar por daños en hardware.

La temperatura adecuada para el correcto funcionamiento de las computadoras debería oscilar entre 15 y 25 °C, aproximadamente, luego para un espacio donde van a trabajar usuarios, una temperatura adecuada sería 22 °C.

Figura 13



Figura 13. Tarjeta para el control de acceso. Reimpreso de Seguridad informática. Copyright 2001 por García Cervigón Hurtado & Alegre Ramos

Figura 14



Figura 14. Sistema de acondicionamiento de aire. Reimpreso de Seguridad informática. Copyright 2001 por García Cervigón Hurtado & Alegre Ramos

Cuando se alcanza una temperatura demasiado elevada, por ejemplo, 40 °C, los procesadores pueden empezar a funcionar mal, además de ser peligrosos para los circuitos. En la BIOS (basic input output system) de los equipos informáticos se pueden programar para que se apague el equipo si la temperatura es demasiado elevada.

2.2 IMPORTANCIA DEL DESEMPEÑO DE MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

Los mecanismos de seguridad de la información serán aplicados y medidos en el problema de la investigación, este conjunto de definiciones, herramientas, controles serán reforzados por la literatura estudiada.

Dado que hablamos de la variable independiente es el foco del estudio medir el grado de mejora del desempeño de los mecanismos de seguridad de la información para aceptar o rechazar las hipótesis formuladas.

2.3 MODELOS DE EVALUACIÓN ASOCIADOS AL DESEMPEÑO DE MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

La variable independiente “Mecanismos de seguridad de la información” definida como:

Tabla 9
Clasificación de la variable independiente

Por su posición:	Independiente
Por su naturaleza:	Cualitativa
Por sus valores:	Discreta
Por sus valores de medición:	Ordinal
Dimensiones:	3

Nota: Elaboración propia.

Sera evaluada a través del modelo de evaluación de Likert, la cual se define como una herramienta para poder cuantificar que haciendo un contraste con las preguntas dicotómicas con respuesta sí/no, nos permite medir actitudes y

conocer el nivel de conformidad del usuario con cualquier afirmación que le planteemos. La escala de medición aplicada será:

- TD: Total desacuerdo
- D: Desacuerdo
- N: Neutro
- A: Acuerdo
- TA: Totalmente de acuerdo

Aplicarla resultaría útil en escenarios en los que queremos que la persona matice su opinión. En este caso, las categorías de respuesta nos servirán para capturar la intensidad de las opiniones del usuario hacia dicha afirmación.

2.4 CONCEPTUALIZACIÓN DE LA PARTICIPACIÓN DEL USUARIO

Conceptualizaremos la variable participación del usuario como el grado de compromiso de las personas involucradas en procesos de los cuales son responsables. La participación del usuario reflejara que tan inmiscuido está el usuario en una acción.

2.4.1 DISEÑO DE SISTEMAS

Según Díaz Harari y Amadeo (2013) indican que el diseño de sistemas por lo general es una tarea compleja, y más aún si cada vez se proponen diseñar

sistemas más variados, más complejos en lo que respecta a tecnología.

Los diseñadores de la interfaz del usuario deben conocer acerca de los efectos del sistema en el usuario, empresa, grupo de trabajo, o en el contexto particular, los diseñadores deben preocuparse acerca de los factores humanos y ergonómicos. Además de averiguar acerca de las mejores representaciones y formas de interacción que va a abarcar el sistema.

Adicionalmente, la interfaz del usuario al ser una parte del software, necesitara para su despliegue de todas las fases del desarrollo de software: análisis, diseño, implementación y evaluación. Al ser un módulo del software que estará en constante manipulación de forma explícita con los usuarios finales y va a interactuar directamente con estos, es importante que estas fases se desarrollen de una manera no tradicional. Dichas fases de desarrollo necesitan que los bocetos de la interfaz sean probados ante los usuarios en forma prematura y aunque estén incompletos, trasladándonos al concepto denominado desarrollo de prototipos, que serán definidos a detalle en tópicos siguientes.

Cuando se inicia el desarrollo de una interfaz, el experto tiene que tener la capacidad de conocer y comprender las peculiaridades de dicho componente de software y mitigar su complejidad mientras se encuentre en vías de desarrollo. Logrando llevar adecuadamente esta fase de desarrollo y ser capaz de sobrellevar las inseguridades que presenta o representaría.

Por ende, podemos definir que el proceso de desarrollo de la interfaz viene caracterizado por los siguientes factores:

- a. Constituye un Proceso Iterativo: Desarrollar la interfaz de usuario implica una serie de pasos constantes e iterativos de mejora continua constante. Como lo explicaremos en adelante, la interfaz del usuario no implica una naturaleza de desarrollo analítica ni secuencial. Mas bien esta necesitara para su despliegue ser analizada frente a actores importantes y modificada de manera sistemática. Es por ello que podríamos decir que es posible adelantar o repetir las etapas de desarrollo según el modelo que se esté diseñando.

- b. Maneja una fase de Requerimientos incompleta: La fase de toma de requerimientos de la interfaz del software generalmente no se efectúa o se da de manera incompleta. Para el usuario es más sencillo dar a conocer las especificaciones computacionales y le resulta difícil expresar requerimientos de visualización, diálogo hombre-computadora. En muy difícil que los usuarios o clientes lleguen a especificar de manera clara lo que necesitan en lo que respecta a elementos de la interfaz, objetos de interacción a utilizar, tipos de feedback, entre otros similares. Entonces, es difícil recibir por parte de ellos una declaración concreta acerca los requerimientos a nivel de la componente de diálogo.

- c. Es de Naturaleza Bottom-up: En contraste del componente de aplicación, en la cual el programador maneja una visión holística de la problemática y desde ese punto procede a subdividirlo en problemas más específicos, el componente de la interfaz tiene su origen desde

distintas partes de información muy puntuales. En un principio, el desarrollador de la interfaz manejará una cantidad considerable de información múltiple, como por ejemplo peculiaridades del usuario, del ambiente, de la aplicación, información de los aspectos tecnológicos, de los estándares del mercado, de equipos para hacer uso del sistema, entre otras informaciones. Esto implica que el desarrollador iniciará a trabajar con datos muy específicos y disímil, por lo que habrá de analizarla realizando generalización, filtrado, abstracción y sintetizado de datos, en pos de aproximarse a un prototipo de diseño del interfaz adecuado.

- d. Requiere un Mecanismo de Representación Especial: La interfaz de usuario debe ser analizada y probada por los distintos tipos de implicados. Podemos encontrar a los usuarios finales que son los destinatarios de la aplicación, los programadores para los cuales se desarrolla el software, también los certificadores que van a certificar el software, como también otra gama de especialistas ideales en tópicos específicos y necesarios como sociólogos, diseñadores visuales, ingenieros electrónicos, etc. También se hace uso de distintas visiones del tema que se complementan entre si. No obstante, cada aspecto tiene líneas que son propios de cada uno, también existen aspectos comunes a trabajar en conjunto. Es por ello, que la interfaz necesita un marco de entendimiento comprendido por todos los implicados, necesita de factores o esquemas representativos más simples, no tan técnicos ni tan formales. Es distinto que la componente de diseño, cuya manera de

representar el diseño debe ser interpretado solamente por el programador, por ende, es posible utilizar diagramas, notas técnicas habituales.

- e. Necesita de Métodos de Diseño Específicos: Como se detalla anteriormente la interfaz del usuario está conformada por componentes como la de presentación, el componente de control de diálogo y la de modelo interfaz-aplicación. Estas engloban factores distintos que han de ser diseñados y desarrollados. Así mismo es totalmente diferente, diseñar los módulos de visualización que diseñar los mecanismos de interacción, o también es diferente diseñar la componente de control de diálogo con el enlace del sistema.

Debido a la variedad de aspectos que implica la interfaz del usuario, es necesario hacer uso de distintos métodos de diseño específicos para cada parte. Por ejemplo, los procedimientos aplicados para el análisis de tareas, definen una secuencia de procesos del usuario y conducta de la interfaz, pero no son eficaces si queremos diseñar el control del diálogo. Opuestamente, la técnica de diagramas de transición y estados o de eventos, definen la interacción y control de diálogo, sin embargo no brindan técnicas de representación para las distintas interfaces del sistema.

- f. Existe una Anticipación de las Etapas de Desarrollo: Durante el desarrollo de la interfaz del usuario se anticipan y abstraen las demás fases de desarrollo. En este escenario la etapa de diseño de la interfaz,

no es posible finalizarla hasta no haberse implementado o por lo menos tener prototipos de la misma. Así mismo la interfaz necesita información de las etapas finales que no es posible conseguir de ninguna otra manera hasta no haber desarrollado el o los bocetos de diseño. Tenemos un panorama similar con la fase de análisis o recopilación de requerimientos. ¿Entonces como saber qué es lo que necesita el cliente a nivel de interfaz, sino puede visualizar bocetos de diseño para ser discutidos? Es por ello que llegamos al escenario donde es necesario estimar el futuro de un prototipo con solo información actual o en tiempo real. La razón de este panorama es que particularmente al hablar de una parte en constante contacto con los usuarios, es común trabajar con información indeterminada, incierta, subjetiva, variable, por todas las fases del proceso de desarrollo, y entonces, es esencial anticipar las fases de diseño o de evaluación para finalizar esta fase.

- g. Prelación de la Etapa de Evaluación: En el caso del desarrollo de los módulos de interfaz de usuario, la etapa de evaluación es primordial para revisar la corrección y estado de avance de las fases anteriores, como fase de toma de requisitos o de diseño de interfaz. En contraste de la componente de aplicación, en la cual la evaluación puede ser dejada para la parte final del de desarrollo, en el caso de la interfaz esta es aplicada en todas las fases.

Es utilizada con el fin de finalizar la fase de toma de requerimientos, para verificar los correctos bocetos de los diseños, para evaluar los

distintos prototipos y también para evaluar los factores de implementación. Esta etapa brinda la facilidad de adecuar la interfaz, cuando no se está tan condicionado por la estructura del sistema. Da la facilidad de afrontar e incorporar correctamente, todos los cambios sugeridos por los usuarios luego de probar la interfaz, siempre y cuando esta se encuentre en su fase de desarrollo.

h. Necesita Participación Activa de los Usuarios: Dado que los factores humanos han de ser considerados en todas las fases de desarrollo, el usuario debe formar parte de manera efectiva y sistemática. Los usuarios deben sentirse comprometidos con las decisiones de diseño, deben ser consultados y se los debe incluir en la totalidad de cada prueba de usabilidad aplicadas en el sistema. El usuario tiene el papel de colaborador en el diseño de las interfaces que serán utilizadas por el mismo, por ende, se podría dar una garantía alta de satisfacción personal. El usuario difícilmente desconfiará si el sistema no es rígido y se ha desarrollado en base a sus preferencias.

i. Implicar ser un Proceso Interdisciplinario: El desarrollo de la interfaz del usuario implica un proceso interdisciplinario, con distintos conocedores en Ingeniería de Software, Factores Humanos, Diseño Visual. Conocedores en Multimedia, Psicología, Comunicación Social, entre otros. Todos ellos con una visión distinta según sus áreas de interés y diferentes lenguajes, sus diferentes visiones, interpretaciones, y por lo tanto puede dificultar su comunicación entre sí. Será necesidad preparar

una metodología con pautas claras de participación y toma de decisiones, con una definición de funciones clara y una coordinación eficiente.

Determinar la Comunidad Destinataria de Lectores:

En la página de la BBC comentan que a la fecha Internet maneja miles de millones de usuarios distribuidos en todo el globo terráqueo. Estos mismos podrían llegar a ser futuros usuarios de la aplicación que se está implementando.

La cantidad de usuarios, el alto grado de heterogeneidad y diversidad entre los mismos, no se debe pasar por alto la modelización de los usuarios. Se hace énfasis en el valor en el diseño centrado en el usuario, enfocándose primordialmente en reducirlo en un grupo más pequeño. Se debe conocer que la mayoría aplicaciones web, son desarrollados pensando en un determinado público, para los cuales se le destina y las funcionalidades desarrolladas, así como los servicios y la información. Pueden ser estudiantes, doctores, clientes, compradores, vendedores, personas mayores.

Así mismo, se debe tener en cuenta que, todo caso de éxito de un sitio, se desarrolla en base a dicho público, es decir cantidad de visitas, permanencia en el sitio del visitante, cookies, numero visitas, ventas, ranking, opiniones, quejas. Por ende, es esencial pensar en ahondar la atención hacia esos usuarios finales, y hacer uso de este análisis, en pos de brindar la mejor experiencia diseño y el más adecuado para estos. Tener información completa acerca de los usuarios finales del sitio, que características tienen y qué es lo

que ellos necesitan hacer en el sitio web y cómo ellos suelen comportarse, no es necesariamente un proceso difícil, y más aún en función de las ventajas que es posible obtener si es que se encara de manera sistemática y consistente. Este proceso básicamente contempla los siguientes pasos:

Tabla 10

ESPECIFICACIÓN DE LA AUDIENCIA DEL SITIO	EXPLICACION
FORMULAR Y RECONOCER LA AUDIENCIA DE USUARIOS	Debido a la masividad de personas que utilizan Internet hay que analizar y definir la audiencia a la que está dirigido el sitio, definiendo perfiles de usuario.
ANALIZAR EL COMPORTAMIENTO ESPERADO DE LA AUDIENCIA	<ul style="list-style-type: none"> -Hay que determinar qué es lo que se pretende que los usuarios realicen dentro del sitio y en qué tiempos. Por ejemplo, si se quiere principalmente que los usuarios entren al sitio a investigar o bajar información, o para comunicarse con otros, o para informarse -Además, analizar si se pretende capturar usuarios temporádicos o permanentes.
MANTENER CONTACTO PREVIO CON LA AUDIENCIA	<ul style="list-style-type: none"> - Es necesario saber que la audiencia debe ser detectada en pos de mantener un contacto directo con ella. Por ello, se deben planificar correctamente citas, encuentros sistemáticos. entrevistados, analizar su entorno y perspectiva. - Si no se puede establecer una comunicación con los usuarios finales del sitio, se puede trabajar con muestras de usuarios, que presenten las mismas características que los patrones considerados en la audiencia.
RECOLECTAR INFORMACIÓN DEL USUARIO	<ul style="list-style-type: none"> - Se debe verificar las hipótesis planteadas sobre los usuarios. - Se debe comprender lo que ellos necesitan de la información, formas de pensamiento sobre organización y agrupamiento de la información, expectativas del sitio, entre otras cuestiones. -Hay que estudiar principalmente cómo son, cuáles son sus niveles de conocimiento sobre la materia. su grado de experiencia con la Web y tipos de sitios similares. - Al trabajar con usuarios, uno puede reunir escenarios

	reales y aprender qué es lo que hace que el sitio Web funcione bien o no.
PARTICIPACIÓN DE LOS USUARIOS INVOLUCRADOS	<ul style="list-style-type: none"> - Permitir que los usuarios ayuden en la construcción del sitio. - Hacerlos participar en decisiones, teniendo en cuenta sus opiniones, críticas y sugerencias. - Explicitar la política de manejo de la información del usuario.

Pasos en la especificación de usuarios destinatarios del sitio web

Nota: Adaptado de Guía de recomendaciones para diseño de software centrado en el usuario; Díaz , Harari, & Amadeo (2013).

Ingeniería de usabilidad

También conocida como calidad de uso, es uno de los objetivos más esenciales en desarrollar las interfases de usuario para un sistema. Esta hace énfasis al grado de efectividad producto de la interacción entre los factores usuario-sistema. Así mismo vela por proveer una interfaz simple, que sea de fácil uso y aprendizaje, además de proporcionar eficiencia y productividad en la utilización e interacción, logrando complacencia subjetiva por parte de los clientes. Esta metodología involucra afrontar las fases de desarrollo de un proyecto en el cual se tienen en cuenta temas de usabilidad desde el inicio hasta el final. A través de este esquema metodológico, se ayuda a los programadores a priorizar su atención en las características de los usuarios y no en las herramientas tecnológicas. Por lo tanto, proporciona un marco definido para una participación efectiva de los usuarios, mejorando la calidad y el trabajo de reingeniería. El cual está formado por un conjunto de procesos, tales como:

- Conocimiento del usuario
- Definición de objetivos de usabilidad
- Análisis heurísticos

- Análisis competitivo
- Diseño iterativo, Diseño paralelo, Diseño participativo
- Diseño coordinado de la interfaz del usuario global
- Prototipación
- Testeo empírico
- Recolección de feedback o información de retorno sobre el uso real del sitio

Algunos procesos requieren cierta explicación, como han de ser:

Tabla 11

Explicación de ciertos procesos de la ingeniería de usabilidad

PROCESOS DE LA INGENIERÍA DE USABILIDAD	EXPLICACIÓN
DEFINICIÓN DE OBJETIVOS DE USABILIDAD	<ul style="list-style-type: none"> *Implica la definición de metas para poder alcanzar la usabilidad *Se incluye como mínimo los objetivos generales de la interfaz.
ANÁLISIS HEURISTICOS	<ul style="list-style-type: none"> *Para alcanzar un grado de usabilidad en un sitio se requiere realizar determinado análisis heurístico como ser: <ul style="list-style-type: none"> -Seguir recomendaciones publicadas -Investigar heurísticas específicas al tipo de interfaz -Utilizar técnicas como testeo empírico
ANÁLISIS COMPETITIVO	<ul style="list-style-type: none"> *Es un proceso en el cual se presentan casos presentes en el mercado, considerando aspectos del diseño y se analizan sus características, ventajas y desventajas
DISEÑO ITERATIVO, PARTICIPATIVO Y PARALELO	<ul style="list-style-type: none"> *Es un proceso que se adecua a la de la Web", donde los sitios se encuentran en constante cambio *La percepción de un usuario de un sistema cambia con el tiempo. El uso del sistema va generando nuevos requerimientos que surgen en función del mismo uso y limitaciones funcionales del sistema antes no detectadas *Se organizan tests de usabilidad para evaluar el sitio frente a usuario, técnicas de focus group para analizar pros y contras *Se analizan y se prueban varias propuestas de diseño *Es un proceso de reingeniería donde el usuario tiene una participación activa

TESTEO EMPÍRICO	<ul style="list-style-type: none"> *Implica el desarrollo de tests evaluativos para medir la adecuación del diseño *Permite fundamentar futuros desarrollos prototipicos *Se emplea durante y al final del desarrollo iterativo
RECOLECCIÓN DE FEEDBACK DE LOS USUARIOS	<ul style="list-style-type: none"> *Hace referencia a seguir obteniendo la participación del usuario una vez que el producto haya sido instalado y puesto en marcha *Es crucial para permitir el rediseño del mismo *Entre las prácticas comunes se encuentran opciones de correo, registro interno de información de usuarios, sugerencias, preguntas frecuentes que realizan, entre otros.

Nota: Adaptado de Guía de recomendaciones para diseño de software centrado en el usuario; Díaz , Harari, & Amadeo (2013).

2.4.2 SISTEMAS INTERACTIVOS

Según Granollers, Lorés vidal y Cañas Delgado (2005) comentan una serie de definiciones de autores destacados del término implicado en el contexto del desarrollo de sistemas interactivos para entender que son los implicados y cuál es su relevancia:

1. Un implicado es cualquier grupo de individuos que podría afectar el cumplimiento de los objetivos de la institución o podría truncar este cumplimiento.
2. Los implicados son aquellos participantes (en el proceso de desarrollo) junto con otros individuos, grupos u organizaciones cuya operación llega a influir o ser influidas por el desarrollo y manejo del sistema de manera directa o indirecta.
3. Los implicados son individuos o instituciones que se verán impactados por el sistema y que tienen influencia directa o indirecta en los requisitos del mismo.

4. El implicado es todo individuo del cual su trabajo se verá afectado, aquel que brinda u obtiene información de esto, o cuya responsabilidad o influencia en la empresa incrementará o disminuirá.

Clasificación

Existen varias propuestas en cuanto a la clasificación de los implicados. La más simple está basada en dividirlos entre los cuales utilizaran el sistema de manera directa o indirecta.

- Ingenieros de software responsables del desarrollo.
- Usuarios finales del sistema.
- Directores de los usuarios que son responsables de su trabajo.
- Los que están relacionados con el desarrollo del sistema.
- Socios y/o proveedores tecnológicos.

Y una de las más detalladas es la que identifica cuatro categorías de implicados:

- Responsables del diseño y desarrollo.
- Personal con interés financiero o económico (responsables de la venta o compra).
- Responsables de su implantación y mantenimiento.
- Personal con interés sobre su uso (los usuarios).

Hay otras clasificaciones de los implicados, pero sea cual sea, en todas queda muy claro que el usuario final de la aplicación es un implicado más. Un implicado directo y muy especial, de ahí que se trate el análisis de sus características en un punto aparte (que a continuación veremos) del conjunto

global de las tareas del análisis de las restricciones.

Identificación

Los implicados por lo general serán identificados personalmente más que por sus roles o funciones, y entre estos son tan importantes los implicados que están estrechamente vinculados en el inconveniente que hay que resolver (por ejemplo, los usuarios finales) así como los implicados en su resolución (por ejemplo, diseñadores del sistema).

Poder identificar a los implicados no resulta una tarea sencilla, en realidad es lo contrario y basándose en ese fin se han desarrollado distintas buenas prácticas.

En cualquier proyecto de desarrollo se puede notar un conjunto de implicados elementales, de los cuales su caracterización es sencilla. Su finalidad es identificar a todos los implicados, inclusive los que podrían influir de manera negativa en el proyecto.

Reuniones con los implicados

Luego de identificar los implicados, se debe proceder a recopilar toda la información relacionada con el proyecto y que es lo que ellos pueden aportar al mismo. Una de las formas más comunes de conseguir dicha información es la planificación de un número de reuniones con los interesados (stakeholders meetings).

Propuesta de Bevan de como se hace una reunión de implicados

- 1) Realizar la planeación de una sesión de un día y hacer partícipes a los interesados con nociones acerca de las intenciones de los usuarios y de su uso, como ha de ser:
 - a) Responsable de negocio (business manager)
 - b) Responsable del proyecto (project manager)
 - c) Usuario (o usuarios) representativos
 - d) Responsables de marketing
 - e) Desarrollador o desarrolladores
 - f) Responsables de la formación
 - g) Responsables del mantenimiento
- 2) Un integrante de la comisión de desarrollo para la reunión desarrollara una lista con todos los tópicos que deben ser tratados en el transcurso de la misma.
- 3) Los preparativos más recomendables a considerar para la reunión programada son:
 - a) Previo a reunirse
 - Seleccionar los temas importantes a revisar.
 - Proporcionar a los participantes con anticipación la lista de temas a tratar.
 - b) En la reunión
 - Luego de tratar los temas clave, se procederá a tratar de obtener un consentimiento en aquellos puntos en los que tenga duda o discrepancia.
 - Si tenemos falta de datos, habrá de recapitular de qué manera se

conseguirá esa información.

- Tener una pequeña sesión para tratar temas secundarios.

c) Luego de la reunión

- Obtener la información faltante.
- Si es que la información no es sencilla de conseguir, se debe organizar una investigación en sitio con el objetivo de analizar a los clientes en su área de labor. Por ejemplo, en un sistema de educación se deberá averiguar cómo se imparte la enseñanza, el aprendizaje y las tareas de apoyo.
- Ofrecer a todos los partícipes de la reunión un documento resumido con las conclusiones de la misma.

Para finalizar este punto, un par de recomendaciones:

1. La reunión se celebrará, si es posible antes de finalizar el proceso de recopilación de requisitos, desarrollar la reunión es importante inclusive cuando el diseño centrado en el usuario se finalizó con cierto retraso o la fase de desarrollo (se tendrá un mayor impacto en el proyecto cuando más tiempo tome en producirse este hecho).
2. Se debe velar por que los interesados asistan a la primera reunión. Las reuniones posteriores deberán desarrollarse de manera más específica con los interesados directamente vinculados con ciertos puntos restantes de detallar.

2.4.3 MEDIDAS ORIENTADAS AL USUARIO

Según podemos comentar con respecto a Martínez Méndez (2004) en medidas orientadas al usuario existe un problema radicando en la relación de las medidas basadas en la relevancia y el usuario que desarrolla la evaluación para el desarrollo hacia otro usuario, las dos medidas tienen su base en el supuesto de que el conjunto de documentos importantes con el objetivo de brindar una respuesta siempre será el mismo. Libremente del usuario que desarrolle el proceso de evaluar. Este escenario claramente no da respuesta a la realidad, ya que distintos usuarios perciben de manera diferente la importancia de qué documento es importante y cuál no lo es. Con el objetivo de brindar solución al problema se define una serie de nuevas acciones en la en cada una se tiene la idea de que los interesados pertenecen a un grupo de similares características y de similar respuesta durante el paso de determinación de la relevancia del resultado de una operación de búsqueda. Este escenario, a pesar de complicado que se desarrolle en la realidad, da la puerta abierta a desarrollar nuevas prácticas definidas como “Medidas Orientadas al Usuario”.

Tenemos tres medidas comunes:

1. Cobertura: Parte de la documentación importante, conocidos que el usuario logrado recuperar.
2. Novedad: Parte de la documentación importante recuperada de las cuales el usuario no tenía conocimiento.
3. Exhaustividad Relativa: La división de la documentación recuperada por

el usuario entre el número de documentos que el usuario pretende revisar.

Es por ello que obtener un valor alto de cobertura significa que el sistema logro encontrar una gran parte de la documentación importante deseada por el usuario. Obtener un alto valor de novedad significa que el sistema maneja una bondadosa cantidad de documentación de la cual no se tenía conocimiento antes.

También existe una medida orientada al usuario conocida como “esfuerzo de exhaustividad”, la cual comprende la diferencia entre la cantidad de documentos importantes esperados a encontrar por el usuario y la cantidad de documentos revisados para encontrar esos documentos importantes. Dicha medida tiene dos ideas base “la colección contiene el número deseado de documentos relevantes y el SRI permite al usuario localizarlos todos”.

Figura 15

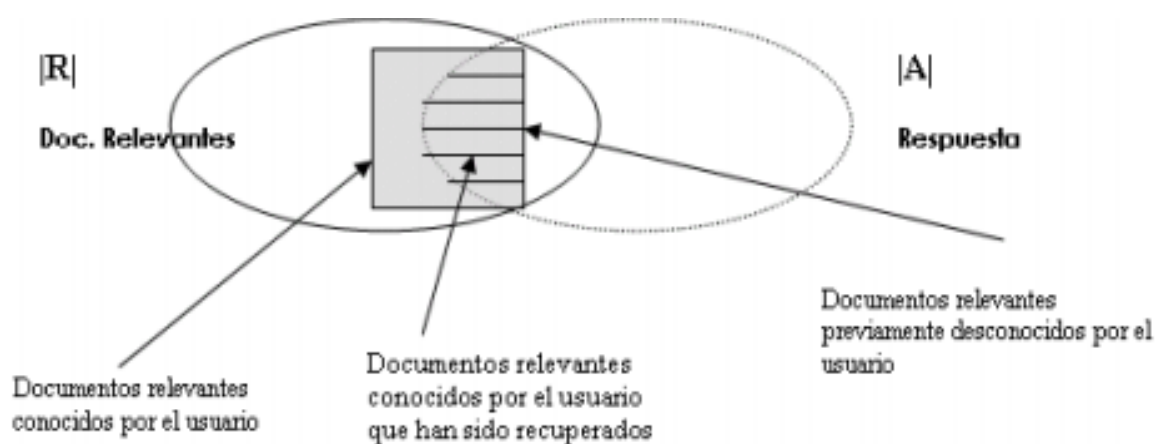


Figura 15. Distribución de documentos relevantes y de documentos integrantes de una respuesta a una operación de búsqueda. Reimpreso de *Recuperación de información*. Copyright 2004 por Francisco

2.4.4 FORMACIÓN DE LOS USUARIOS

Según Fernández Alarcon (2006) la formación de los usuarios quiere decir que la capacitación y apoyo a los usuarios son partes que se deben desarrollar de manera paralela y si fuera posible antes de implementar un sistema nuevo. Los puntos de capacitar o formar a los usuarios y al apoyo como soporte es crucial para tener un proyecto exitoso.

Por lo general se separa la capacitación y soporte a los usuarios del sistema de manera independiente. Pero se da que ambas están fuertemente relacionadas, dado que ambas tienen la misma finalidad: lograr que los usuarios del sistema tengan la capacidad de sacar el máximo provecho de manera eficiente a las prestaciones del sistema.

Formación de los usuarios en un nuevo sistema

Actualmente tenemos distintas modalidades para la capacitación de usuarios: los estudios de manera presencial, los estudios a distancia y la educación auto aplicada a través de recursos multimedia. Acorde al escenario actual, el especialista en desarrollo de sistemas deberá elegir un método teniendo en cuenta los recursos, la importancia del sistema de información y de la experiencia de los usuarios.

Posibles temas potenciables que deben ser impartidos a los usuarios de sistemas:

- Usabilidad del sistema nuevo
- Tópicos generales sobre tecnología
- Tópicos acerca de sistemas de información
- Tópicos organizacionales
- Gestión del sistema a implementar
- Proceso de instalación del nuevo sistema

Luego de que el especialista termine de analizar y decida la lista de temas importantes para los usuarios del sistema nuevo, el especialista seleccionara los métodos que se utilizaran.

Algunas modalidades de mayor aceptación eso es la de los usuarios expertos. Dicho método define en que los usuarios finales suelen manejar más confianza entre sus compañeros que con los especialistas para aprender cómo usar el sistema, los usuarios expertos manejan conocimiento del funcionamiento e importancia de las operaciones diarias con la tecnología que se encuentra implementando. Dicho método se puede aplicar luego de que el especialista en sistemas seleccione un grupo de personas que sean estimados por los demás usuarios y capacitarlos con la finalidad de llegar a que sean expertos en temas del uso del sistema. A continuación, los usuarios formados y expertos tendrán el objetivo de formar a sus compañeros para el correcto manejo del sistema de información.

Otra modalidad muy popular es la formación a través de herramientas multimedia. En esta modalidad el cliente es quien interactúa con la herramienta electrónica a diferencia de la formación habitual (que se centra solo en recibir

el mensaje) aquí hay más dinámica para el usuario ganando más participación y es más interactiva. Sin embargo, esta forma de capacitar en base a herramientas multimedia tiene el límite en la cantidad de respuestas solidas que ofrece a los usuarios.

Podemos también nombrar a los talleres de formación o seminarios, los cuales están basados en distintos especialistas explicando cómo funciona el sistema. En esta modalidad el asistente maneja un rol pasivo dado que el personaje principal es el docente especialista que imparte sus conocimientos al público y los estudiantes se limitan a tomar notas.

El manejo de software como guía también es usado para la capacitación de los usuarios. En este escenario la capacitación se realiza a través del nuevo sistema, ejemplo de ello podemos nombrar las aplicaciones de ofimática como Word que permite pedir ayuda en un menú específico para hacer consultas acerca de su uso.

Otra modalidad que podemos comentar son los seminarios o talleres multimedia, los cuales son un híbrido entre los seminarios convencionales y las herramientas de software multimedia. Estos se caracterizan por manejar varios especialistas con el objetivo de explicar las principales funciones del sistema y definir como debe funcionar a los usuarios. En este escenario el papel principal es para los usuarios finales dado que ellos serán quienes interactúen con el sistema en cambio el especialista profesor es solo un guía de capacitación.

Finalmente, de manera adicional se puede capacitar a los usuarios subcontratando a una empresa especializada en este rubro. A veces es

posible que la información nos la proporcione el proveedor que ha vendido la solución de software y hardware. Y en otros casos existen especializadas en la capacitación de usuarios a herramientas de software.

2.4.5 RECURSOS HUMANOS Y TI

Según Giner de la Fuente (2004), indica en los recursos humanos. Los elementos descritos hasta aquí son elementos materiales, obviamente necesarios para el proceso de conversión de datos en información. Pero nada de todo lo descrito sería posible sin el concurso de los recursos humanos, que constituyen una pieza esencial para diseñar y desarrollar los sistemas de información para cubrir las más diversas necesidades.

En la actualidad, para poder construir sistemas de información con ayuda o apoyo de las TIC, es necesario el concurso de un conjunto de profesionales con variados conocimientos.

Tabla 12

Los recursos humanos del sistema de información y sus competencias

Los clientes de la información	Son los que dan validez y valor a la información
Director/Jefe Proyecto	Trabaja en equipo
Consultor de Negocio	Orientado al cliente
Consultor Tecnológico	Comunicación
Técnico de Sistemas	Capacidad analítica
Analista Funcional	Visión global
Técnico de Diseño	Toma decisiones
Gestor de Contenidos	Orientado a la innovación/cambio
Analista Programador	Orientado a resultados

Nota: Adaptado de Los sistemas de información en la sociedad del conocimiento, Giner de la Fuente (2004)

La tabla 12 pone de relieve los distintos tipos de recursos humanos que son necesarios para construir sistemas de información con apoyo o soporte de las

TIC, así como las diferentes competencias que en conjunto deben poseer y manejar. Dentro de los recursos humanos necesarios, se pueden distinguir claramente dos tipos de personas:

- Los usuarios finales del sistema de información, en síntesis, los clientes para los cuales se construye el sistema de información. Estos individuos no tienen necesidad de tener conocimientos o capacidades específicas y profundas en materia tecnológica. Lo que sí deben de conocer con precisión es qué es lo que desean que haga el sistema, qué requerimientos de funcionamiento o de suministro de información deben cumplir.
 - Si lo que se necesita son informes, los usuarios de la información habrán de precisar con detalle qué modelo de información desean, qué elementos son críticos a medir, cómo medirlos, cómo relacionarlos y luego de cuánto tiempo.
 - Si lo que se va a querer es automatizar procesos a través de un sistema de información, deberán precisar, diseñar, el flujo de información de la nueva función o proceso una vez incorporada.
 - Es evidente que, para acometer esta labor de diseño, bien sea de los datos convenidos en información (modelo de información), bien de los datos convenidos en instrucciones para automatizar un proceso (rediseño de procesos), podrán y deberán contar con las personas especializadas del área informática y telecomunicaciones. Pero deberán ser ellos los que asuman la responsabilidad y el avance del proyecto. Esta responsabilidad

de lo que se quiere que sea el proyecto, ya sea de información o de rediseño de procesos, no puede ni debe delegarse en otros. Es el cliente, el usuario del sistema de información, el que debe asumirla.

- Aquellos que podríamos identificar como "los obreros del sistema". Éstos son un conjunto de personas, que pasaremos a detallar a continuación, las cuales ponen en juego sus diferentes conocimientos y competencias para poder construir los sistemas de información deseados por los clientes finales de la información, mediante el soporte o la ayuda de las TIC:

En cuanto a las competencias a poseer por ambos grupos de personas, básicamente las podríamos resumir en una capacidad para poder trabajar en equipo. En: necesaria una interrelación constante de saberes de diferente tipo. lo que obliga a estas personas a trabajar de forma conjunta y coordinada. De aquí se derivarán las otras competencias: capacidad de comunicación, visión global y analítica, orientado al cliente (al que solicita y necesita el sistema de información), establecimiento de propuestas innovadoras, capacidad para tomar decisiones y poder obtener resultados en tiempo y presupuesto.

2.4.6 COMPUTACIÓN DEL USUARIO FINAL

Según McLeod Raymond (2000) indica en la computación de usuario final como aspecto estratégico, que no todas las personas que realizan computación de usuario final tienen el mismo nivel de cultura computacional. Es posible clasificar a los usuarios finales en cuatro categorías con base en sus conocimientos de computación.

Usuarios finales a nivel de menús: Algunos usuarios finales no pueden crear su propio software, pero se comunican con software prescrito mediante menús como los del software para Mac y Windows.

Usuarios finales a nivel de macros: Algunos usuarios finales cuentan con conocimientos de uso de software prescrito que van más allá de la selección de opciones de menú. Estos usuarios finales pueden usar el lenguaje de macros (comandos) del software para realizar operaciones aritméticas y lógicas con los datos. Por ejemplo, los usuarios de Microsoft Excel pueden usar macros especiales para realizar procesos que no pueden efectuarse empleando sólo los menús.

Usuarios finales programadores: Algunos usuarios finales pueden usar lenguajes de programación como BASIC o C++, y pueden crear programas a la medida, programas que satisfacen sus propias necesidades.

Personal de apoyo funcional: En algunas empresas, los especialistas en información son miembros de unidades funcionales, no parte de un departamento de servicios de información. Este personal de apoyo funcional consiste en especialistas en información en todos los sentidos de la palabra, pero están adscritos a sus áreas de usuario específicas e informan a sus

gerentes funcionales.

Dos ingredientes clave caracterizan los cuatro niveles de capacidad de los usuarios finales. Primero, todos los niveles pueden crear aplicaciones; segundo, ninguno de ellos es miembro de la unidad de servicios de información.

Tipos de aplicaciones de usuario final

Hasta aquí, la EUC ha afectado los principales subsistemas de CBIS en diversos grados. Casi todas las aplicaciones de computación de usuario final han estado limitadas a:

- Sistemas de apoyo a decisiones (DSS) relativamente sencillos.
- Aplicaciones de oficina virtual que satisfacen necesidades individuales

Esto deja a los especialistas en información con la responsabilidad de trabajar con los usuarios para desarrollar:

- Aplicaciones de AIS y MIS
- DSS complejos
- Aplicaciones de oficina virtual que satisfagan las necesidades de la organización
- Sistemas basados en conocimientos

En tanto continúe esta variabilidad en el impacto de la EUC, como seguramente sucederá, siempre habrá necesidad de especialistas en información.

Beneficios de la computación de usuario final

La EUC beneficia a la empresa de dos maneras principales: equipan las capacidades de quien hace el desarrollo con los retos del sistema y elimina o reduce la brecha de comunicación entre el usuario y el especialista en información.

- **Equipar capacidades y retos**

El desplazamiento de la carga de trabajo de desarrollo de sistemas a las áreas de (OHMIO liben a los especialistas para que se concentren en los sistemas organizacionales y complejos. y les permite desempeñar mejor su trabajo en estas áreas. Además, los especialistas tienen más tiempo que dedicar al mantenimiento de los sistemas existentes, un área de responsabilidad que es muy importante.

- **Reducción de la brecha de comunicación**

Un problema que ha perseguido al desarrollo de sistemas desde los primeros días de la computación ha sido la comunicación entre el usuario y el especialista en información. El usuario entiende el área problema mejor que la tecnología computacional. El especialista, en cambio, es experto en la tecnología, pero no en el área problema. Al dejar que los usuarios creen sus propias aplicaciones, deja de existir la brecha de comunicación, ya que no hay necesidad de comunicarse. Por lo mismo, si los usuarios desarrollan una porción de sus sistemas, la brecha se reduce.

Ambos beneficios dan como resultado la creación de mejores sistemas que los

producidos por especialistas en información que tratan de realizar la mayor parte del trabajo ellos mismos.

Riesgos de la computación de usuario final

Los beneficios de la EUC tienen un precio. Cuando los usuarios finales crean sus propios sistemas, exponen a la empresa a varios riesgos.

Sistemas mal dirigidos: Los usuarios finales podrían aplicar la computadora a aplicaciones que deberían trabajarse de alguna otra manera, digamos manualmente.

- **Sistemas mal diseñados y documentados:** El grupo de usuarios finales a pesar de que manejen un alto nivel cultura de tecnologías de la información, será imposible manejar la experticia de los ingenieros de software en lo que implica a diseñar el sistema de información. Además, con los cortos tiempos que se manejan por poner el sistema de información en producción, los usuarios finales suelen no poner énfasis a la documentación de los diseños del sistema, esto resulta crucial para un correcto mantenimiento del mismo.
- **El manejo ineficiente de los recursos de información:** Si no existiese una gestión centralizada del software y hardware, la empresa seguramente administrara mal sus recursos de adquisición de estos. Por ejemplo, podrían adquirirse diferentes marcas de computadoras personales que no pueden vincularse para formar una red y comprarse varias copias de software cuando podría compartirse una sola copia. Además, los usuarios podrían 'reinventar la rueda' atando sistemas que ya se han desarrollado.

- Integridad de datos corrupta: Es posible que los usuarios finales cometan errores a la hora de guardar datos en las distintas bases de datos de la organización. Es posible que otros usuarios realicen trabajos usando estos datos erróneos. En consecuencia, tenemos información corrupta que puede desencadenar en una toma de decisiones no acertadas.
- Pérdida de la seguridad: Al igual que el anterior punto, hay la probabilidad de que los usuarios finales descuiden sus datos y su software. De que manejen sus contraseñas de papeles y estos lleguen a un basurero desde su escritorio, es así como se puede vulnerar la seguridad de estos usuarios de manera sencilla. Y dejando la posibilidad de que los hackers accedan al sistema con sus cuentas y realicen actos que afectarían a la empresa.
- Pérdida de control: Los usuarios diseñan sistemas con el fin de solucionar sus propias necesidades asilándose de algún plan que solucione las necesidades de la empresa. Es un riesgo enorme manejar distintos sistemas de información separados por áreas.
- La computación de usuario final en perspectiva: La computación aplicada al usuario final es un fenómeno que no va a desaparecer. Si acaso, su influencia aumentará. En vista de los beneficios potenciales, la empresa debe crear un plan estratégico de los recursos de información que permita a la EUC crecer y florecer. En cuanto a los riesgos, es preciso aplicar a las áreas de usuarios los mismos tipos de controles que han funcionado tan bien en servicios de información.

2.4.7 IMPLICACIÓN E INFLUENCIA DEL USUARIO

Según Laudon y Laudon (2004) la implicación e influencia del usuario. La acción de implicar e involucrar al usuario en diseñar y manejar los sistemas de información tiene distintos resultados efectivos. Primeramente, cuando los usuarios son muy participes diseño de los sistemas, ellos aumentaran sus oportunidades de modelar el sistema acorde a sus necesidades y requisitos de negocios y más oportunidades de manejar el resultado, luego será más posible que reaccionen positivamente al sistema terminado dado que han participado constantemente en el proceso de desarrollo. Concentrar los conocimientos y la habilidad en los usuarios mejorara la solución.

Debido al uso extendido de internet y del manejo de herramientas de cuarta generación, los usuarios actuales están tomando un papel de liderazgo en la integración de la adopción, desarrollo e implementación de las innovaciones de tecnología de la información. No obstante, con frecuencia los usuarios Tienen un enfoque muy estrecho y limitado del problema que se planea resolver y es posible que pasen por alto importantes factores tecnológicos o soluciones alternativas del sistema de información. Aun se requieren las destrezas y visión de los diseñadores profesionales de sistemas, más o menos de la misma manera que se necesitan los servicios de un arquitecto para construir una casa nueva.

Por lo general, el especialista y el cliente manejan una relación dificultosa en el proceso de implementar el sistema de información. Los especialistas y

usuarios manejan distintas prioridades así antecedente e intereses. Esto es conocido como la brecha de comunicaciones entre el diseñador y usuario. Dichas diferencias llevan a lealtades organizacionales, métodos de resolución de problemas y vocabularios divergentes. Por ejemplo, por lo general los especialistas de sistemas de información manejan una alineación muy específica o mecanizada del problema a resolver; están en búsqueda de resultados distinguidos y complejos en los cuales la eficacia del hardware y el software juegan un papel primordial a costa de la facilidad de uso o de la eficiencia organizacional.

Los usuarios gustan de sistemas que se orienten a resolver problemas de negocios o a facilitar las tareas de la empresa. Comúnmente, las prioridades de ambos grupos son tan desiguales que parecen hablar idiomas diferentes. Podemos ver estas diferencias en la tabla 13, que muestra las preocupaciones típicas de los usuarios finales y los especialistas técnicos (diseñadores de sistemas) con respecto a desarrollar un nuevo sistema informático.

Los usuarios finales y los diseñadores de sistemas manejan usualmente problemas de comunicación, estos problemas son una razón importante de la importancia de los requisitos del usuario cuando no se recopilan adecuadamente para el sistema de información provocando comúnmente indiferencia de parte de los usuarios de la fase de implementación.

Tabla 13
Preocupaciones típicas de los usuarios y especialistas técnicos

Preocupaciones del usuario	Preocupaciones del diseñador
¿El sistema produce la información que necesito para trabajo?	¿Cuánto espacio de almacenamiento en disco consumirá el archivo maestro?
¿Qué tan rápidamente puedo acceder a los datos?	¿Cuántas líneas de código de programa se llevará ejecutar esta función?
¿Qué tan fácilmente puedo recuperar los datos?	¿Cómo podemos reducir el tiempo en la CPU cuando se ejecuta el sistema?
¿Cuánto apoyo de oficina necesitaré para introducir datos en el sistema?	¿Cuál a la manera más efectiva de almacenar estos datos?
¿Cómo se ajustará la operación del sistema con mi programa diario de negocios?	¿Qué sistema administrativo de bases de datos debemos usar?

Nota: Adaptado de *Sistemas de información gerencial*, Laudon & Laudon (2004).

Siempre existirá un riesgo alto de que el proyecto de desarrollo fracase si existiese un contraste notable entre usuarios - especialistas y mientras estos grupos busquen objetivos diferentes. En tales condiciones, con frecuencia a los usuarios se les deja fuera de la implementación. Como no tienen la capacidad de comprender el mensaje de los especialistas, los usuarios suelen tomar la decisión de dejar el desarrollo del proyecto totalmente a los especialistas en desarrollo de sistemas. Tomando en cuenta todo el trabajo de implementación y que tenga base en consideraciones técnicas es esperable que estos sistemas fracasen en satisfacer las necesidades de la empresa.

2.4.8 SATISFACCIÓN DEL USUARIO

Según la satisfacción del usuario en relación al funcionamiento y a los atributos de un sistema de información de Rey Martin (2000), está vinculada de manera directa con el manejo del sistema. Cuando los usuarios renuncian usar el sistema de información y buscan otras soluciones da lugar a un nivel de satisfacción bajo. Inversamente también podemos decir que el nivel de uso del sistema es una métrica de satisfacción del usuario del sistema usado, especialmente si se da el caso de que el sistema es de uso opcional y no obligatorio, como un sistema de biblioteca virtual.

Podemos entender cuando hablamos de satisfacción de los usuarios en sistemas de información, como el grado en que los usuarios consideran que el sistema cumple con sus requerimientos. Un usuario satisfecho es el resultado que el sistema tiene esperado lograr, y espera crear un sentido de dependencia al mismo sus las funciones ofrecidas.

La satisfacción del usuario contempla también el tiempo invertido, los recursos, si fuera el caso y el nivel de esfuerzo o sacrificio, sin embargo, debe ser el usuario el que defina o le dé un valor al grado de satisfacción, partiendo de la unión de dos aspectos como la prestación del servicio y el sacrificio, y podemos clasificar este balance en:

***Sacrificio elevado/prestación de servicio modesta:**

Este balance tiene como consecuencia la satisfacción mínima del usuario, existe una mala insatisfacción máxima o nivel de satisfacción mínimo, se

obtiene un valor bajo de valoración de parte de los usuarios y puede dar cabos sueltos a reclamos y sugerencias para la empresa

***Sacrificio modesto/prestación modesta:**

Define un nivel bajo de satisfacción o insatisfacción media, como consecuencia la opinión del servicio será inestable y con inseguridad sobre la posibilidad de volver a usar el servicio.

***Sacrificio elevado/prestación elevada:**

Provoca un nivel de satisfacción incluso, justamente por eso la opinión el juicio es casi positivo. La duda para volver a usar el servicio es baja, ya que significa ganas de volver a manejar el sistema.

***Sacrificio modesto/prestación elevada**

Define el mayor nivel de satisfacción, la opinión es puramente verdadera y por ende significa la mayor confianza en volver a usar el sistema. Por ende, con este balance se obtiene algo mayor a satisfacción se logra la confianza, si es que el usuario confía en el sistema continuara haciendo uso de el llevando a una fidelización del usuario.

Figura 16

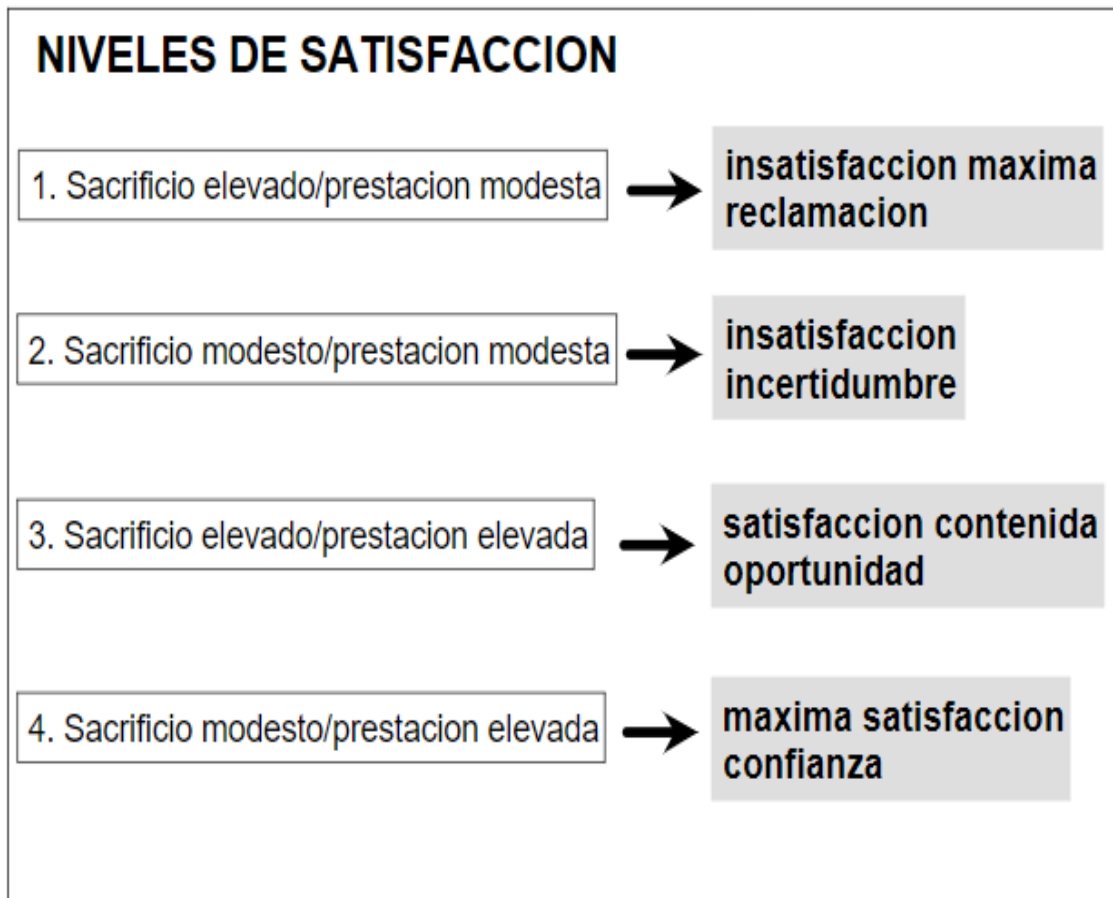


Figura 16. Niveles de satisfacción del usuario. Reimpreso de La satisfacción del usuario; Un concepto en alza. Copyright 2000 por Carina Rey Martin.

2.5 IMPORTANCIA DE LA PARTICIPACIÓN DEL USUARIO

La participación del usuario será medida y evaluada con la variable independiente para medir su correlación.

Se consideró la variable participación del usuario ideal para el estudio de correlación a través de la observación, estudio de bibliografía y juicio crítico del investigador.

2.6 MODELOS DE EVALUACIÓN ASOCIADOS A LA PARTICIPACIÓN DEL USUARIO

La variable dependiente “Participación del usuario” definida como:

Tabla 14
Clasificación de la variable dependiente

Por su posición:	Dependiente
Por su naturaleza:	Cualitativa
Por sus valores:	Discreta
Por sus valores de medición:	Ordinal
Dimensiones:	5

Nota: Elaboración propia.

Sera evaluada a través del modelo de evaluación de Likert, la cual se define como una herramienta para poder cuantificar que haciendo un contraste con las preguntas dicotómicas con respuesta sí/no, nos permite medir actitudes y conocer el nivel de conformidad del usuario con cualquier afirmación que le planteemos. La escala de medición aplicada será:

- TD: Total desacuerdo
- D: Desacuerdo
- N: Neutro
- A: Acuerdo
- TA: Totalmente de acuerdo

Aplicarla resultaría útil en escenarios en los que queremos que la persona

matice su opinión. En este caso, las categorías de respuesta nos servirán para capturar la intensidad de las opiniones del usuario hacia dicha afirmación.

2.7 CONCEPTUALIZACIÓN DE LA PLANIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Conceptualizaremos la variable planificación de los sistemas de información como el grado de compromiso de la empresa en establecer los pasos a seguir en un determinado periodo de tiempo para implementar un sistema de información en la empresa.

2.7.1 PLANIFICACIÓN DE SISTEMAS

Según Ramon Rodríguez, García Mínguez y Lamarca Orozco (2007) la planificación de sistemas indica que planificar es establecer qué hay que hacer, quién lo realizara, con cuanto tiempo y con qué recursos, para cumplir una meta. El plan de proyecto es la principal herramienta para ello, como la libreta de bitácora, utilizada por un gestor de proyecto para asegurar lograr los objetivos deseados.

Un plan de proyecto se puede considerar:

- Un mapa de ruta estructurado que establece todas las actividades que hay que hacer con el fin de lograr las metas de la empresa.
- Una definición de los tiempos y recursos –tecnológicos y de negocio– necesarios para completar el trabajo.
- Una herramienta para monitorizar avances, controlar el alcance y gestionar el proyecto con la finalidad de asegurar los resultados dentro del umbral de tiempo y presupuesto definidos al inicio.
- Un medio para informar los progresos y implicar a los participantes del proyecto.

Planificar proyectos es, en definitiva, estructurar y describir las actividades requeridas para lograr los objetivos del proyecto, teniendo en cuenta las responsabilidades y recursos requeridos en cantidad, tipología y experiencia.

Existe una máxima en las carreras de motor que dice que ganar una décima de segundo al tomar una curva de manera bien planificada puede suponer más

de un segundo al salir de la misma. Planificar en sistemas un proyecto correctamente supone una inversión para ahorrar tiempo en su ejecución.

Además, la planificación permite mejorar la calidad, ser eficiente y mejorar las perspectivas del proyecto a largo plazo.

Finalmente, pero no en último lugar, el plan es un instrumento de comunicación y diálogo, con el cliente y dentro del equipo de trabajo.

Un resumen de las ventajas que ofrece la planificación estructurada de un proyecto informático es posible verlo en la figura 17.

Figura 17

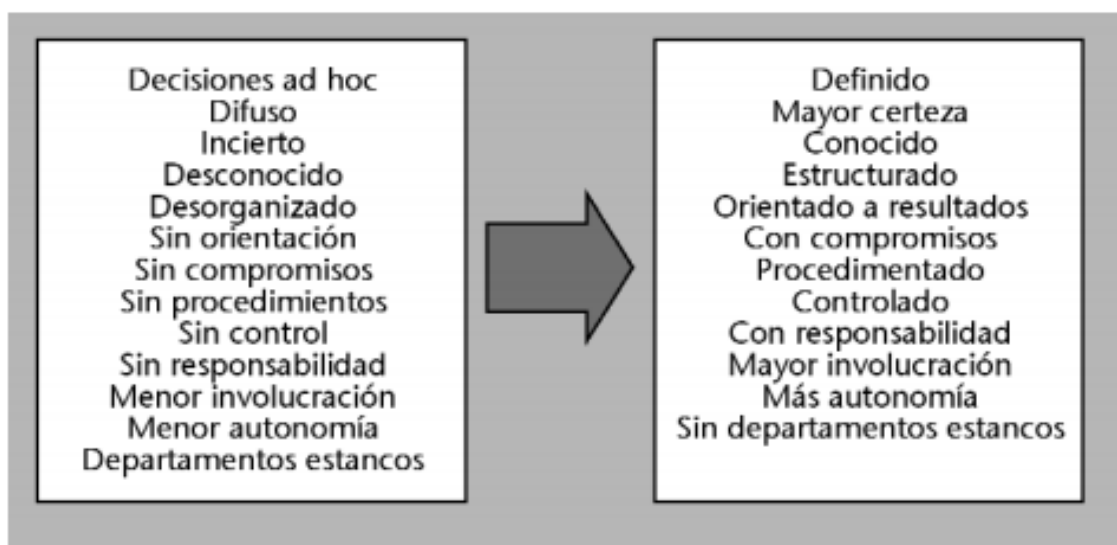


Figura 17. Características de un proyecto planificado. Reimpreso de *Gestión de proyectos informáticos*.
Copyright 2007 por Ramon Rodríguez, García Mínguez, & Lamarca Orozco.

Sin embargo, la planificación de proyectos no puede ni debe considerarse un proceso estático. Por el contrario, como veremos en el capítulo siguiente referido a la ejecución del proyecto, es un ciclo en constante revisión.

Contenidos del Plan

El plan de un proyecto debe contemplar todos los elementos siguientes:

- Los objetivos y los resultados esperados para el del proyecto, de manera que permita la evaluación del éxito o fracaso del proyecto, tal como se han descrito en los capítulos anteriores.
- Los hitos principales del proyecto, coincidentes con puntos de decisión, entregables, finalización de etapas, etc. Una definición más detallada de hito se establece en los apartados siguientes del capítulo.
- Los mecanismos de control del alcance del proyecto, y de gestión de cambios en éste.
- La involucración de los distintos agentes participantes en el proyecto, sus roles y responsabilidades.
- La definición de las actividades del proyecto, es decir las tareas o grupos de tareas de las que se compone, los recursos necesarios y el resultado o hito que debe obtenerse mediante la realización de estas actividades.
- El calendario de trabajo, con los tiempos de realización según la fecha de inicial y la fecha final de todas las actividades y la de cada uno de los hitos.
- La organización y el equipo asignado al proyecto, con la matriz de roles y responsabilidades para los diferentes hitos y actividades.
- El presupuesto del proyecto, con las estimaciones de inversión y coste presupuestadas a partir del consumo de recursos, su previsión de evolución a lo largo del tiempo de duración del proyecto y la previsión

de beneficios esperados.

- El sumario de las asunciones realizadas sobre los riesgos identificados previamente a la implantación del proyecto, su posible impacto sobre el plan de proyecto y el plan de gestión de estos riesgos.
- La calidad de los trabajos realizados, según los resultados funcionales y operacionales esperados y la definición de las condiciones y principios de aceptación de los mismos.

2.7.2 SISTEMAS Y MECANISMOS

Según el estudio del sistema de información y los mecanismos de seguridad informática en la pyme de Solano Rodríguez, García Perez y Jesus Bernal (2016), realizar una correcta gestión de la seguridad de la información implica definir políticas, herramientas de control y de monitorear el sistema. Estas acciones deben ser implementadas en la gestión de la empresa a través de una correcta planificación de tecnologías de la información en la institución.

Los altos mandos de la organización deberán presentar un mayor interés por la eficacia, liderazgo y soporte a los procesos relacionados con la gestión de la tecnología.

La implementación de las políticas de seguridad informática comprende la definición de roles, la definición de acciones y procesos involucrados en la seguridad de la información. La ISO 27000 define un grupo de buenas prácticas y estándares acerca de la seguridad de la información. Estas buenas prácticas luego de ser integradas al quehacer diario de los usuarios logran una mejor implementación de los sistemas de información y un mejor monitoreo del control de los sistemas.

Cuando la dirección organizacional de la empresa proporciona facilidades a las tareas que comprende el desarrollo de proyectos tecnológicos logran desarrollar una mejor prevención a los riesgos de los sistemas de información llegando a minimizar su impacto. Y cuando la organización ofrece un apoyo efectivo, el nivel de riesgo se minimizará para las inversiones de tecnologías de la información.

La planificación de los sistemas es una fase de los proyectos de TI, es un componente importante para lograr una correcta implementación de los sistemas. Esta comprende parte del desarrollo del sistema como la toma de requerimientos de los usuarios, análisis del sistema, diseño y la gestión de recursos.

Realizar la planificación como utilidad de gestión favorecerá el desarrollo de las tecnologías de la información, así como su correcto encaminamiento con los requisitos de la empresa. Así mismo favorece a la correcta conclusión de proyectos de tecnología y mejorar el nivel de calidad de los sistemas.

2.7.3 METODOLOGÍA DE SELECCIÓN

Según el estudio metodología para selección de sistemas ERP de Chiesa (2004) en presentación y planificación general del proyecto, señala que durante esta fase se debe realizar un cronograma de implementación genérico contemplando principalmente fechas de actividades (inicio y fin) y ser presentado a las partes involucradas.

También se deben presentar macros de procesos que contemplen recursos coordinar los recursos de proveedores, como:

- Construcción de las áreas de trabajo, así como la instalación del sistema. Durante este proceso el proveedor de ERP juega un rol importante, así como el personal de soporte y usuarios de la empresa. Se deben definir las fechas y tiempos necesarios, así como recursos necesarios y sus proveedores.
- Luego de haber realizado la instalación del producto y la construcción de las áreas de trabajo, pasa lugar a los especialistas de seguridad de la información que armaran la estructura y permisos para los usuarios.
- En paralelo la empresa consultora debe empezar a desarrollar la documentación necesaria para los usuarios.

Durante el periodo de planificación se suelen tener tiempos muy variados (desde cortos hasta prolongados) acorde a las demoras que se puedan presentar en las coordinaciones con los proveedores y su disponibilidad de recursos para las necesidades de planificación. Para finalizar esta fase se deben de presentar la documentación necesaria a todos los usuarios, incluyendo un cronograma de actividades a grandes rasgos y fechas de inicio y

fin de trabajo.

2.7.4 SISTEMAS Y PLANIFICACIÓN

Según Serpbell Bley y Alarcón Cárdenas (2015) indican que el concepto de sistemas y la planificación, en los años 1940-1950 se desarrolló una nueva perspectiva para la solución de problemas complejos de ingeniería. La existencia de un problema fue considerada como un vacío (necesidad) en el entorno y la solución para remover este vacío fue enfocada como un sistema.

Por ejemplo, ante la necesidad del transporte surge el automóvil; ante la necesidad de coordinación surge la planificación en la ejecución de los proyectos. Luego, se procede a presentar un análisis que explicará la planificación y como se inserta dentro de la perspectiva de sistemas, como parte de un sistema más global que es el sistema de Administración de Proyectos. Este análisis es importante por la comprensión de que los proyectos son sistemas abiertos, con una gran cantidad de interfases que deben administrarse en forma integrada, de modo de asegurar que se logren los objetivos del proyecto. Es decir, la administración de proyectos es en la práctica la administración de un tipo de sistemas y requiere por tanto una visión global para que sea realizada en forma efectiva. Como se verá posteriormente, muchas de las herramientas y métodos de la planificación han sido desarrollados dentro de este marco de referencia.

Un sistema es un conjunto de objetos, principios, reglas, etc., unidos por una interacción ordenada para formar un todo organizado, sujeto a restricciones que limitan las respuestas de los componentes individuales y del sistema. Un esquema simple se presenta en la figura 18.

Figura 18

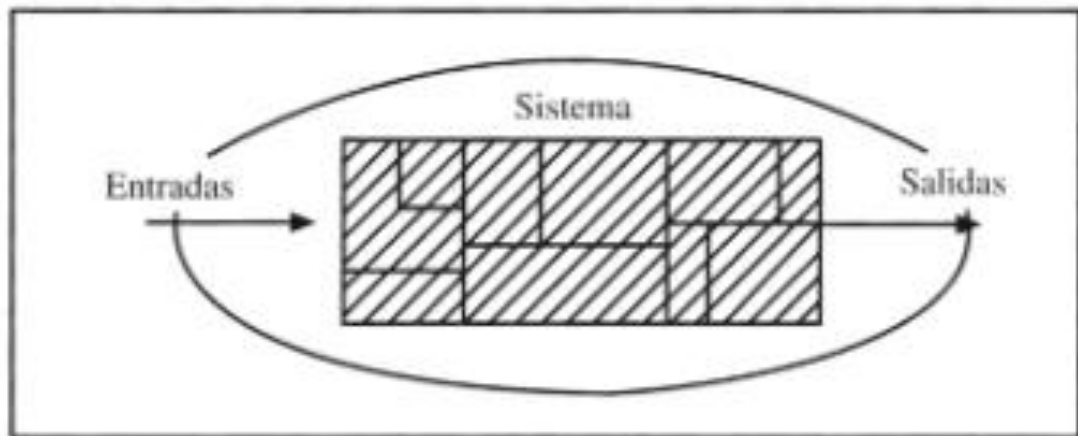


Figura 18. Sistema genérico. Reimpreso de Planificación y control de proyectos. Copyright 2015 por Serpbell Bley & Alarcón Cárdenas.

Para satisfacer una necesidad utilizando el esquema de sistemas, deberíamos de realizar las siguientes acciones:

1. Análisis de la necesidad o problema a resolver.
2. Definición y especificación del problema.
3. Desarrollo del criterio de diseño que permita obtener una solución.
4. Generación de las alternativas de solución.
5. Verificación de la factibilidad física, económica y financiera de las soluciones.
6. Optimización de alternativas factibles.
7. Evaluación de las alternativas optimizadas y selección de la mejor solución.
8. Implantación de la solución.
9. Retroalimentación y control para mejorar en forma continua.

Los pasos o etapas indicadas anteriormente corresponden de manera inequívoca a las etapas propias de la realización de un proyecto como se verá

más adelante. Es decir, tal como se mencionó anteriormente, los proyectos nacen como resultado de la existencia de una necesidad o problema que una organización debe resolver.

Un sistema también puede mirarse como una estructura piramidal (figura 19), basado en el concepto de que los componentes, relacionados en forma lógica, forman subsistemas, y la unión de estos subsistemas en diferentes combinaciones, forman sistemas.

Figura 19

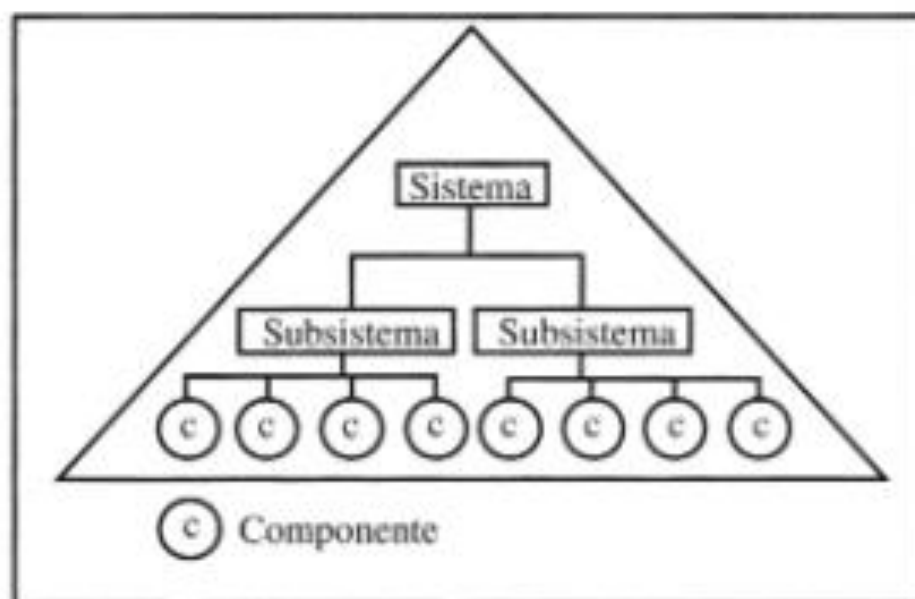


Figura 19. Tipo de estructura de un sistema. Reimpreso de Planificación y control de proyectos. Copyright 2015 por Serpbell Bley & Alarcón Cárdenas.

Existen entonces tres procesos básicos en la creación de un sistema:

1. Los componentes básicos son sintetizados para formar parte de un sistema, que generalmente tiene una estructura piramidal, con subsistemas y componentes.

2. Se analiza el sistema o solución para asegurar su factibilidad y optimización.

3. Selección, implantación y modificación de este sistema.

El proceso de planificación se ha desarrollado en forma análoga a la metodología de diseño de sistemas. La planificación constituye un subsistema del sistema de administración de Proyectos, así como lo son las otras funciones de la administración como la organización, la dirección y el control, así como podemos ver en la figura 20. Es decir, la administración de proyectos es un sistema que usa las funciones indicadas para transformar los recursos de un proyecto tales como recursos humanos, materiales, equipos y otros en un resultado que se mide generalmente en función de su desempeño en costo, plazo, calidad y satisfacción de los interesados.

Figura 20

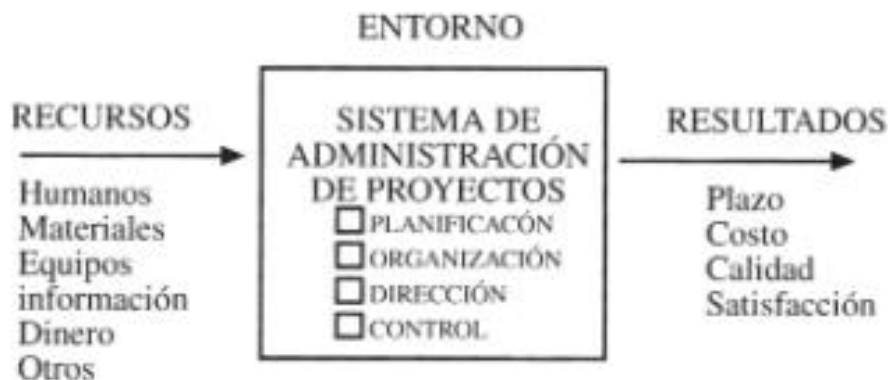


Figura 20. Planificación dentro de la administración de Proyectos. *Reimpreso de Planificación y control de proyectos. Copyright 2015 por Serpbell Bley & Alarcón Cárdenas.*

Mientras se desarrolla la planificación de un proyecto también se sigue un esquema similar al proceso de desarrollo de un sistema, siendo este último procedimiento directamente aplicable a esta función.

1. Definir metas u objetivos para el proyecto con relación a necesidades o problemas existentes.
2. Considerar las amenazas o restricciones existentes para realizar el proyecto.
3. Considerar oportunidades disponibles para la realización del proyecto.
4. Considerar diversas opciones o alternativas para realizar el proyecto.
5. Construir un modelo o plan para la ejecución de acuerdo a las alternativas disponibles.
6. Seguir el progreso de la ejecución del proyecto.
7. Revisar el modelo de acuerdo a la información de seguimiento.
8. Tomar acciones de control.

En la aplicación del enfoque de sistemas a la planificación y control de proyectos hay que reconocer tres atributos de este concepto:

1. Enfatiza la importancia de las relaciones que unen los componentes en una entidad concreta.
2. Utiliza una metodología determinada.
3. Aplica las herramientas y técnicas de diseño de sistemas apropiadas a la etapa del proyecto y a las necesidades dictadas por el tamaño y complejidad del proyecto.

Haciendo un paralelo entre el diseño de sistemas y el proceso de la planificación, podemos subdividir este último en distintas etapas como son:

1. Análisis y definición: este es el primer paso dentro de la planificación. Es necesario analizar detalladamente el proyecto para lograr una primera subdivisión y determinar los alcances de éste. Luego de concluir esta etapa se abran definido las generalidades del proyecto y la lista de tareas que se desarrollaran.
2. Planeamiento: estando ya determinadas las actividades que se desarrollaran para el proyecto, es necesario determinar una secuencia lógica para la ejecución de éstas. Primeramente, se organizarán las tareas (priorizar y ordenar según su importancia), para luego secuenciarlas obteniendo un cronograma correcto.
3. Programación: en esta etapa se debe determinar los tiempos y manejo de recursos de las tareas, logrando un programa detallado.
4. Evaluación y optimización: Para obtener que el programa sea el más adecuado se debe de realizar un estudio de recursos al margen de uno de costos y tiempo. Optimizando los datos anteriores para obtener el más alto beneficio, se obtiene el programa final.
5. Implantación: consiste en poner en marcha el cronograma de trabajo.
6. Seguimiento: Es el primer paso que se debe seguir para controlar efectivamente el proyecto. Implica también recopilar datos acerca de cómo desarrolla el proyecto teniendo en cuenta los tiempos y costos de las tareas.
7. Control: Implica la comparación de la información del presente con el cronograma principal, y revisar que diferencias existen entre ambos para ser corregidas.

8. Actualización: Se desarrollarán cambios al cronograma principal con la finalidad de ejercer un mejor control.

En la figura 21 se muestran estas actividades y la secuencia de etapas del proceso.

Figura 21

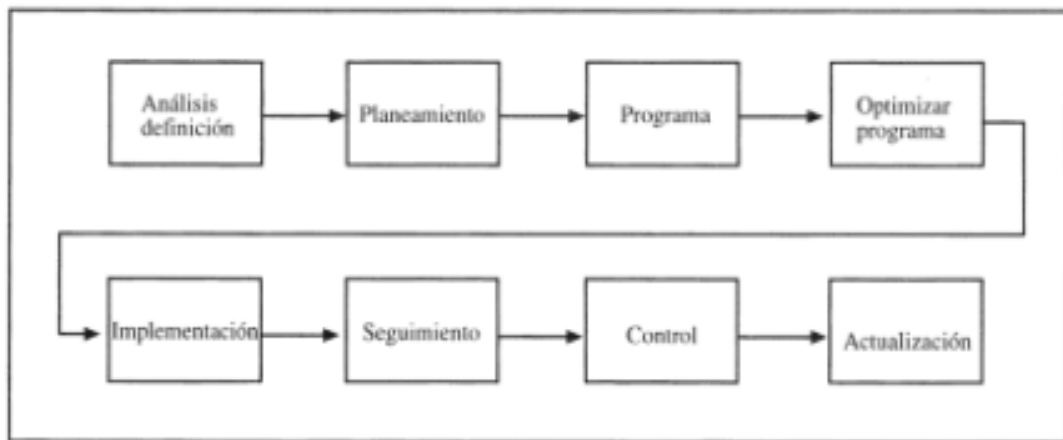


Figura 21. Proceso de Planificación. Reimpreso de Planificación y control de proyectos. Reimpreso de Planificación y control de proyectos. Copyright 2015 por Serpbell Bley & Alarcón Cárdenas.

2.7.5 PLANIFICACIÓN ESTRATÉGICA DE SI

Según Fernández Alarcon (2006) la planificación estratégica de sistemas de información, es la cual ubica y establece necesidades sobre las tecnologías de la información y sus aplicaciones para las principales necesidades de la organización. Es por ello que un plan estratégico de sistemas de información (PETI) proporciona el marco de trabajo adecuado para la implementación de sistemas, los pasos a seguir, consideraciones y métodos de evaluación.

El proceso de tomar decisiones para decidir que la finalidad de los sistemas de información comprende cuatro etapas o fases. La primera fase explica el surgimiento del estudio de la informática en las empresas durante los años setenta. Durante esos tiempos la informática y sus aplicaciones eran usadas por lo general por las áreas de facturación y contabilidad, debido a su sencilla implementación. A lo largo de esta fase era común que se desarrollara un sistema de información apenas un área o departamento lo necesitaba, era así demostrando la nula planificación o un PETI.

En la segunda fase tenemos un aumento indiscriminado de solicitudes de atención por parte de las áreas usuarias. Las solicitudes de aplicaciones informáticas iban en aumento dado que los problemas eran cada vez más complejos producto de las limitantes de recursos de las áreas de tecnología o informática. Es por ello que era forzoso establecer criterio para seleccionar y priorizar adecuadamente las necesidades, no obstante, dichos criterios se solían desalinearse con los objetivos estratégicos de la organización e iban alineados más bien a los requisitos de las áreas usuarias solicitantes.

Figura 22

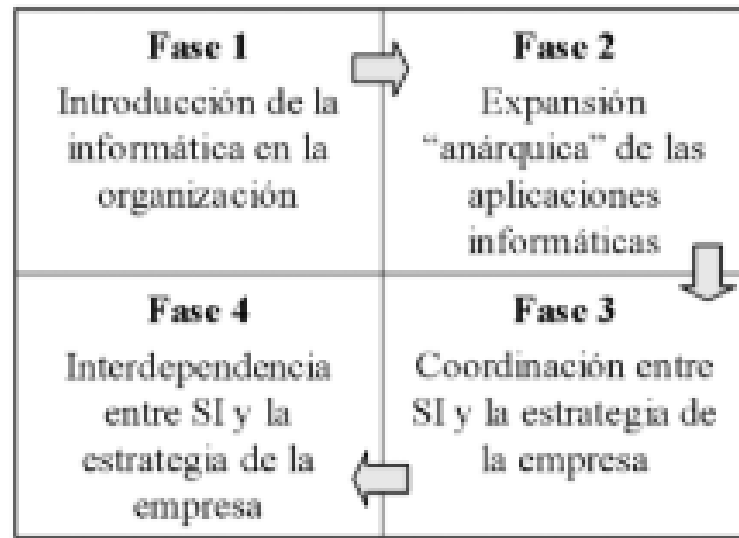


Figura 22. Evolución de la planificación estratégica de sistemas. Reimpreso de Desarrollo de sistemas. Copyright 2016 por Vicenç Fernández Alarcon.

La tercera fase implica la concesión de recursos para poder desarrollar los sistemas de información alineados a los objetivos de la empresa. Los altos cargos de la empresa establecen ideas que ayudaran a identificar y priorizar el desarrollo de proyectos de tecnologías de la información alineados a los objetivos de la empresa. Y esta es la razón por la cual lo llamamos PETI o plan estratégico de tecnologías de la información.

Adicionalmente otro objetivo de esta etapa define la infraestructura en común y marco de trabajo para todas las implementaciones que comprenda las tecnologías de la información.

La última etapa o cuarta etapa define la interdependencia estratégica de la empresa con los sistemas de información, que implica el desarrollo de un PETI como parte de la planificación empresarial.

2.7.6 FUNCIONES GERENCIALES

Según McLeod Raymond (2000), las cinco funciones gerenciales: planificar, organizar, proporcionar, dirigir y controlar. Estas funciones se llevan a cabo en el orden dado, y el plan es la base para todas las actividades subsecuentes.

Realizar una planificación a largo plazo además se define como planificación estratégica, dado que haciendo una correcta planificación se podrá definir los objetivos a largo plazo de la empresa que favorecerá su posición, llevando a la capacidad de poder establecer una estrategia para llegar a dichos objetivos.

La importancia de la planificación estratégica a nivel gerencia superior es claramente la razón por la que Roben Anthony bautizó ese nivel como nivel de planificación estratégica.

Cuando una empresa organiza a sus ejecutivos en un comité ejecutivo, este grupo siempre asume la responsabilidad de la planificación estratégica.

Planificación estratégica funcional

Si la empresa por lo general está implicada en realizar una planificación estratégica, notaran de la obligación para que todas los departamentos o áreas definan su plan estratégico. Estos planes independientes se conocen como planes funcionales que definen la manera de como las áreas aportaran a la empresa con el cumplimiento de sus objetivos estratégicos.

La estrategia de enfocar la planificación estratégica funcional es que cada área defina su propio plan independientemente al margen de las demás. Sin embargo, este enfoque no garantiza que las áreas trabajarán unas con otras como subsistemas sincronizados. Podemos apreciar en la figura cómo deben

trabajar los departamentos o áreas funcionales para lograr una correcta planificación estratégica.

Figura 23

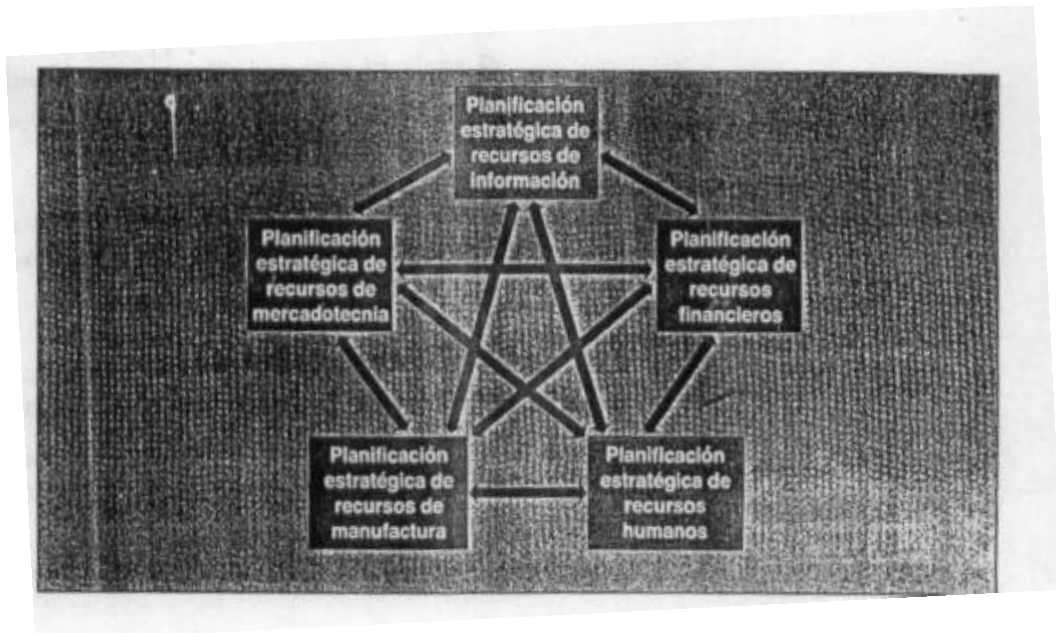


Figura 23. Relación entre las áreas y procesos de planeación. Reimpreso de *Sistemas de información gerencial*. Copyright 2000 por Jr McLeod Raymond.

Los flujos de información y de influencia están simbolizados por las flechas.

Planificación estratégica de recursos de información

Últimamente es posible que el área de tecnologías de la información estén más relacionadas con la planificación estratégica de todas las áreas de la empresa. A esta dependencia se le conoce como 'transformación de conjuntos de estrategias' y a lo largo de los años se le conoce como 'planificación estratégica de recursos de información'.

Transformación de conjuntos de estrategias

Una vez que el área de tecnologías de la información empezó a implementar

los planes estratégicos, el proceso empezaba por elaborar estos planes alineándolos de manera especial a los objetivos de la organización, conocido también como conjunto de estrategias organizacional.

Luego como siguiente paso e independiente del anterior, se debería crear el plan de servicios de información para soportar a los objetivos de la organización. El plan de servicios de información se definió conjunto de estrategias, objetivos, restricciones y estrategias. Dicho enfoque, denominado transformación de conjuntos de estrategias, podemos apreciarlo en la figura 24.

Un defecto básico de la transformación de conjuntos de estrategias es que las áreas funcionales no siempre cuentan con los recursos necesarios para asegurar el cumplimiento de los objetivos importantes de la organización. Sin embargo, varias compañías, algunas de las cuales han tenido un éxito considerable, siguen adoptando este enfoque.

El enfoque SPIR

Una posible solución a los escenarios de falta de recursos de información es la de la planificación estratégica de recursos de información o también conocida como (SPIR, strategic planning for information resources). En el momento que una organización adopta SPIR, los planes estratégicos organizacionales y de las tecnologías de información se ejercen de forma paralela. El plan de la organización manifiesta de cuales servicios de información puede abastecer, y el plan de servicios de información define las futuras necesidades para las tecnologías de la información. Podemos apreciar como se ilustra la forma en

que cada proceso de planificación influye en el otro en la figura 25.

Figura 24

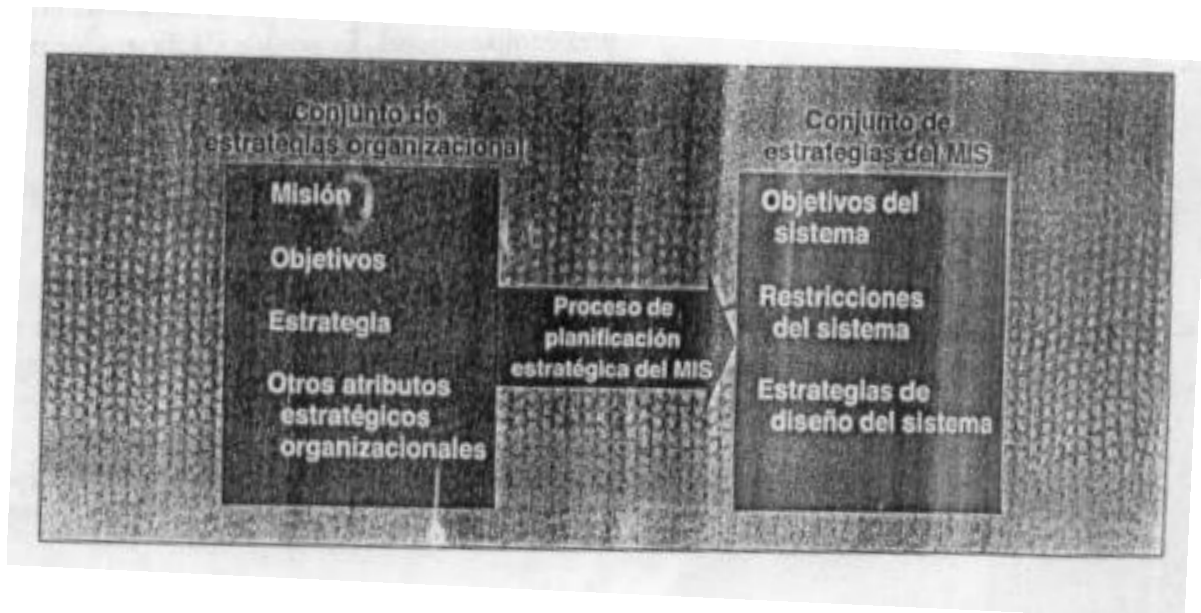


Figura 24. Transformación de conjuntos de estrategias. Reimpreso de *Sistemas de información gerencial*. Copyright 2000 por Jr McLeod Raymond

Figura 25

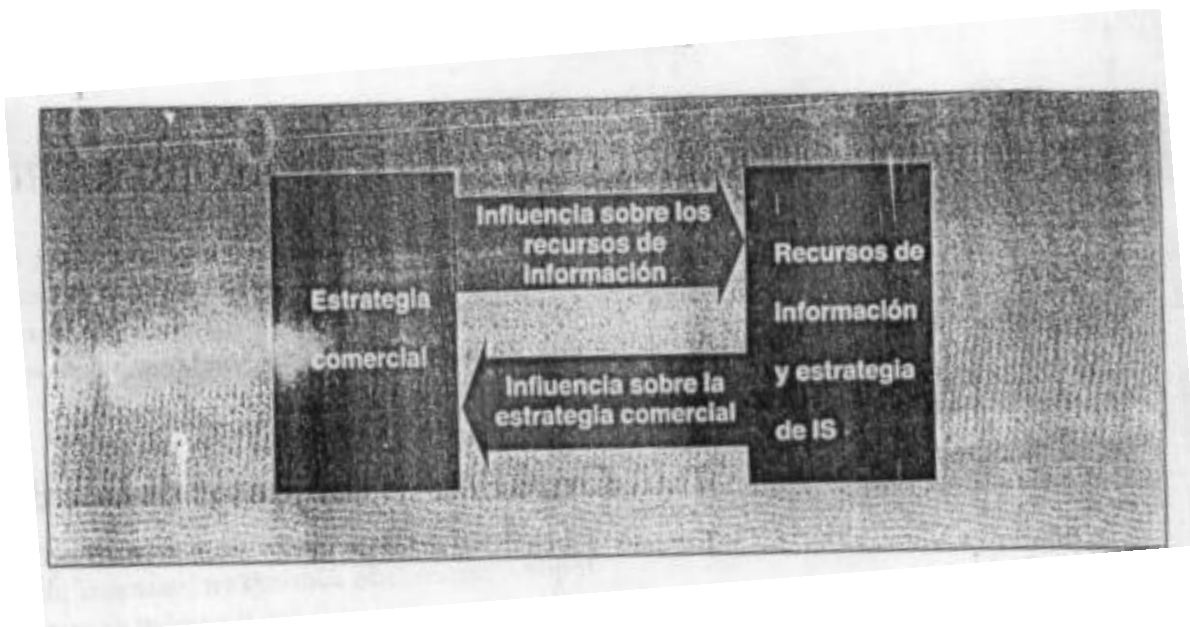


Figura 25. Influencia entre procesos de planificación. Reimpreso de *Sistemas de información gerencial*. Copyright 2000 por Jr McLeod Raymond

Contenido de un plan estratégico de recursos de información

Las organizaciones desarrollan un plan estratégico de recursos de información para cumplir sus necesidades de tecnologías de la información. Sin embargo, se han identificado algunos tópicos críticos que deben incluirse. Básicamente dicho contemplara: (1) la lista de objetivos de se espera cumplir para todos los subsistema en el transcurso que dure el plan, y (2) los recursos de información que se necesitaran para conseguir esa lista. Este contenido es posible apreciarlo en la figura 26.

Figura 26

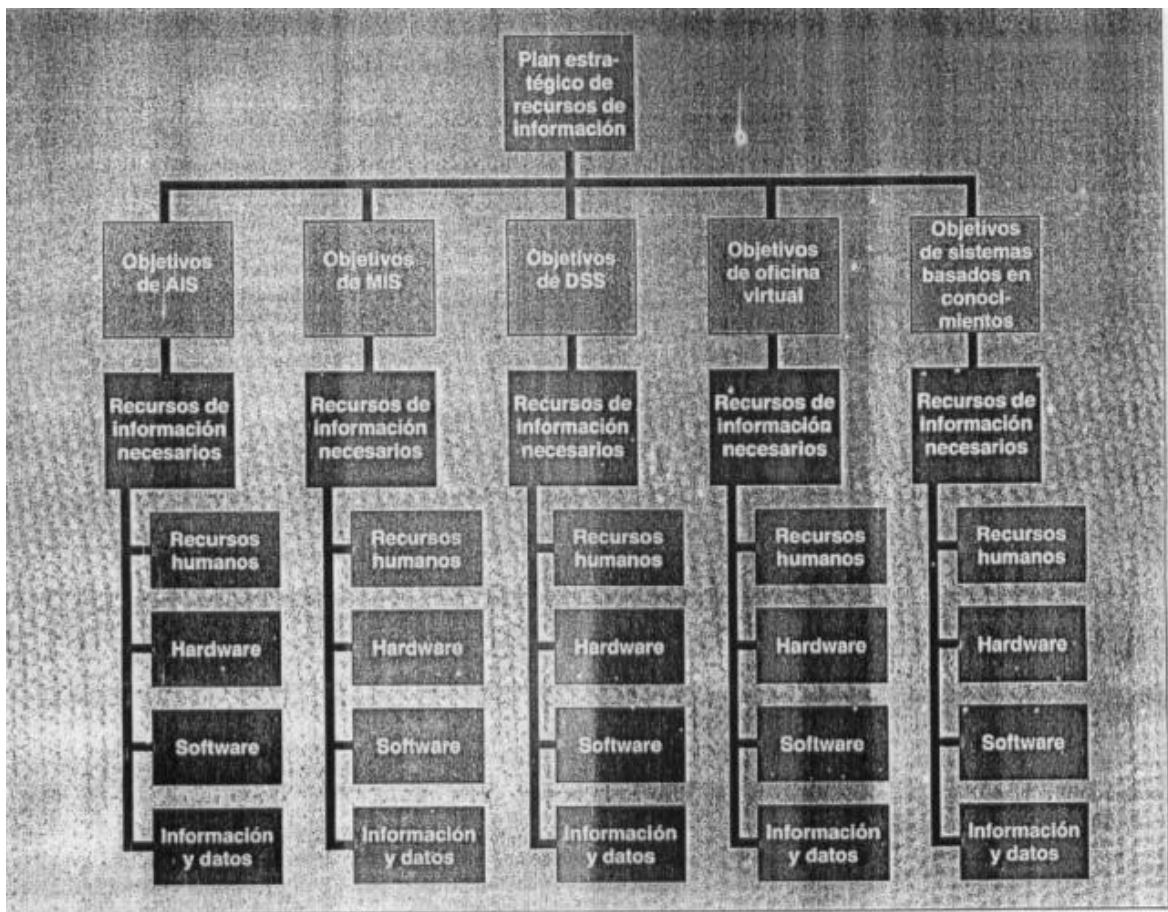


Figura 26. Marco de referencia básico de un plan estratégico de recursos de información. Reimpreso de *Sistemas de información gerencial*. Copyright 2000 por Jr McLeod Raymond

Como ejemplo de la forma en que el plan puede considerar las necesidades de un subsistema dado del CRIS, suponga que un sistema de inventarios se va a modificar para poder surtir los pedidos de los clientes con mayor rapidez. La agilización se logra ubicando los artículos de inventario en la bodega de tal manera que los surtidores de pedidos recojan los artículos de los anaqueles en la secuencia más eficiente posible.

El siguiente paso del proceso de planificación es identificar los recursos de información que se necesitarán para lograr el objetivo.

La figura 27 presenta una muestra de cómo pueden detallarse los objetivos y las necesidades de recursos. Se estudia detenidamente el papel que los usuarios desempeñarán en el proyecto. Esto tiene especial importancia cuando se espera que los usuarios realicen parte de la labor de desarrollo, o toda.

Figura 27

Sistema:	Inventarios.
Subsistema:	Disposición física de una bodega.
Objetivo:	Implementar un programa para el 1o. de octubre del próximo año que determine la ubicación de los artículos en la bodega para optimar el surtido de pedidos. El programa se ejecutará cada trimestre.
	<i>Necesidades de recursos</i>
Hardware:	Aproximadamente dos horas de mainframe por trimestre, lo que incluye mantenimiento y prueba de programas. La configuración de mainframe requiere aproximadamente 20 MB de espacio en disco, una terminal con teclado, una impresora de líneas y un graficador.
Instalaciones:	Usar las instalaciones existentes.
Software:	Programa de programación lineal modificado que contemple una interfaz tanto gráfica como tabular. Las necesidades de codificación estimadas son de 1 000 líneas.
Base de datos:	Usar el archivo maestro de inventario existente.
Especialistas en información:	Aproximadamente 18 meses-persona de tiempo de desarrollo por parte de personal de servicios de información, repartidos como sigue: analista de sistemas (6), administrador de bases de datos (4), programador (6), operador de consola (2). Además, el personal de los sistemas de bodega contribuirá con aproximadamente dos meses-persona.
Información:	Los empleados de existencias de bodega requieren un código de ubicación en bodega en los vales de bodega. El código está incluido en el registro maestro de inventarios.
Usuarios:	El personal de los sistemas de bodega proporcionará a servicios de información diseños de todas las pantallas más una especificación de la función objetivo y una lista de todas las restricciones en notación matemática. El gerente requerirá dos días de capacitación práctica en el uso del sistema, administrado por un miembro del personal de los sistemas de bodega. Servicios de información proporcionará el manual de usuario.

Figura 27. Ejemplo de plan estratégico de un sistema de inventarios. Reimpreso de *Sistemas de información gerencial*. Copyright 2000 por Jr McLeod Raymond.

2.7.7 COMPROMISO ADMINISTRATIVO

Según Laudon y Laudon (2004) el compromiso administrativo, define que todo proyecto de tecnologías de la información debe contar con el soporte y responsabilidad de la administración de la empresa todos sus niveles. Será altamente posible que los involucrados (usuarios y personal especializado) lo adopten positivamente. Los dos grupos tendrán claro el papel de su participación durante la fase de desarrollo generará atención y reconocimiento del nivel más alto y serán reconocidos por el tiempo y esfuerzo brindado. Además, el apoyo administrativo contempla el apoyo de recursos y fondos hacia las tecnologías de la información para garantizar su éxito.

Adicionalmente la relación entre la metodología de trabajo, procesos y todo cambio empresarial con el nuevo sistema depende de la participación de la administración de la empresa. Cuando un directivo establece la priorización de una necesidad de sistemas de información, es más factible que sus dependientes le den ese trato al sistema.

Nivel de complejidad y riesgo

Los sistemas se diferencian drásticamente por distintos factores como alcance, limitaciones, alcance y características de la organización. Es probable que algunos proyectos de desarrollo de sistemas fracasen o sufran problemas de tiempo dado que tienen distintos niveles de riesgo entre sí.

La estructura del proyecto de tecnología de la información y su respectiva capacidad técnica, alcance, integrantes y tamaño influye en la gestión del riesgo del proyecto.

- **Dimensiones del proyecto**

Mientras el proyecto aumente de tamaño como se refleja en sus recursos invertidos, la cantidad de las personas involucradas y el tiempo comprendido para la implementación y el número de unidades empresariales afectadas— mayor será el riesgo a contemplar. Los grandes proyectos de tecnologías de la información manejan una probabilidad de fracaso de 50 a 75% a diferencia de otros proyectos debido a que estos proyectos suelen ser complicados de controlar. Las características conductuales del sistema, quién maneja el sistema y como este se encuentra relacionado con los procesos de negocios, contribuyen a la dificultad de los grandes proyectos de sistemas tanto como las peculiaridades técnicas a saber, la cantidad de código usado en la programación, tiempo invertido en el proyecto y el presupuesto.

- **Estructura del proyecto**

Algunas etapas de un proyecto manejan una mejor estructura que otras. Contemplan requisitos más entendibles y puntuales de manera que los resultados puedan completarse de manera sencilla. El grupo de usuarios tiene conocimiento de lo que necesitan y que es lo que esperan que haga el sistema; cuando existe una baja probabilidad para que los requisitos sufran cambios, los proyectos manejarán un menor riesgo en contraste con los que tienen requerimientos ambiguos , indeterminados y en constante cambio; obteniendo resultados que no se pueden definir.

- **Experiencia con tecnología**

Obtendremos un riesgo elevado para el proyecto si al equipo del proyecto y al personal del sistema de información les falta la capacidad técnica. Si el equipo se encuentra poco capacitado en lo que respecta a hardware, software del sistema, software de aplicaciones o sistema de gestión de bases de datos usado en el proyecto, existe una alta probabilidad de que ese proyecto tome más tiempo en finalizar o tenga problemas de implementación debido al desconocimiento de la tecnología.

Administración del proceso de implementación

Desarrollar un nuevo sistema implica que se deba administrar y orquestar de manera cuidadosa. Comúnmente se omiten algunos elementos que son básicos para su éxito, como capacitar correctamente asegurando que los usuarios finales se estén cómodos con sistema implementado y que tengan completamente claro su funcionalidad, es un tema que se suele mientras se desarrolla la implementación de un sistema de información. Cuando se maneja un presupuesto limitado en un principio, es probable que en la fase final de un proyecto no existan recursos suficientes para entrenamiento y documentación. Los conflictos y las inseguridades inherentes a cualquier esfuerzo de implementación se exaltarán en el caso de que un proyecto de implementación se administre y organice de manera deficiente. Existe una alta posibilidad de que un proyecto de tecnologías de la información tenga las siguientes consecuencias cuando no se administre correctamente:

- Costos que superan a los presupuestos.

- Retrasos de improviso para cumplir los tiempos.
- Déficits técnicos que reflejan un bajo desempeño a lo esperado.
- Fracaso en obtener resultados anticipados.

¿Por qué están mal gestionados los proyectos? Los proyectos del sector privado por lo general están acotados a la mitad en lo que respecta al presupuesto y tiempo requerido para realizar la entrega del sistema finalizado acorde al cronograma. La mayoría de proyectos son entregados con funcionalidad incompleta.

Lamentablemente el 80% de los proyectos de software supera a sus presupuestos, con el proyecto de software "promedio" rebasando el 50% por encima del presupuesto. Aproximadamente el 30 y 40% de todos los proyectos de software suelen ser "clandestinos", es decir que exceden con mucho el cronograma y las proyecciones de presupuesto originales no se desarrollan como se especificó en un inicio. ¿Por qué existen proyectos con una tan mala administración y qué puede hacerse al respecto? A continuación, establecemos algunas sugerencias:

- Ignorancia y optimismo: Las herramientas para establecer la cantidad de tiempo que se necesita para analizar y diseñar los sistemas están desarrolladas de manera incorrecta. Las aplicaciones en su mayoría son "primerizas" (eso significa que no existe una experiencia previa en el área de aplicaciones). Mientras más grande sea el sistema de información, mayor será la probabilidad de manejar un de ignorancia y

optimismo. El fruto de estos factores resulta en estimaciones que suelen ser optimistas “en el mejor escenario” y equivocadas “se supone que todo marchara bien” pero en la realidad eso no es así.

- El mítico mes-hombre: La medida para proyectar costos más comúnmente utilizada por los diseñadores de sistemas viene a ser el mes-hombre. Esta define que los proyectos se estiman en base a cuántos meses-hombre se necesitan. No obstante, agregar más trabajadores a los proyectos no implica necesariamente la reducción del tiempo transcurrido, necesario para finalizar un proyecto de sistemas. A diferencia de la cosecha de algodón en la que las tareas se pueden dividir rígidamente, no se requiere la comunicación entre los participantes ni es necesario entrenarse con frecuencia, desarrollar sistemas de información implica tener una visión clara de la relación entre las tareas y estas se pueden realizar de manera separada, es necesario tener una comunicación constante capacitación extensiva. Aumentar el personal cuando algunos proyectos manejan tareas independientes por lo general puede un retraso en la entrega de las mismas, llevando a un aumento de los costos de comunicación, capacitación y coordinación desencadenando un bajo resultado para los partícipes. Para efectos de comparación, ¿se imagina lo que pasaría si se agregaran cinco espectadores aficionados a un equipo de baloncesto profesional en un juego de campeonato? El equipo compuesto por cinco jugadores profesionales de baloncesto probablemente se desempeñaría mucho mejor a cono plazo que el

equipo con cinco profesionales y cinco aficionados.

- Quedándose atrás: las malas noticias viajan lentamente

En la gran mayoría de proyectos en todos los campos. Por lo general la demora en completar los objetivos, estado de algunas tareas y e incertidumbres no se comunican a los gestores del proyecto hasta que llega a ser demasiado tarde. El proyecto CONFIRM, un proyecto de sistemas de información a muy grande escala para integrar reservaciones de hoteles, de aerolíneas y de automóviles en arriendo, es un ejemplo clásico. Fue patrocinado por los Hoteles Hilton, Budget Rent-A-Car y la corporación Marriott y desarrollado por AMR Information Services, Inc., una subsidiaria de American Airlines Corporation. El proyecto era muy ambicioso y técnicamente complejo, empleando a un equipo de 500 personas. Los miembros del equipo de administración del proyecto de CONFIRM no se presentaron inmediatamente con la información exacta cuando el proyecto empezó a tener problemas con la coordinación de varias actividades del procesamiento de transacciones. Los clientes siguieron invirtiendo en un proyecto vacilante porque no estaban informados de sus problemas con la base de datos, su rol en la toma de decisiones y tecnologías de integración.

2.8 IMPORTANCIA DE LA PLANIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN

La Planificación de los sistemas de información será medida y evaluada con la variable independiente para medir su correlación.

Se consideró la variable Planificación de los sistemas de información ideal para el estudio de correlación a través de la observación, estudio de bibliografía y juicio crítico del investigador

2.9 MODELOS DE EVALUACIÓN ASOCIADOS A LA PLANIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN

La variable dependiente “Planificación de los sistemas de información” definida como:

Tabla 15
Clasificación de la variable dependiente PS

Por su posición:	Dependiente
Por su naturaleza:	Cualitativa
Por sus valores:	Discreta
Por sus valores de medición:	Ordinal
Dimensiones:	5

Nota: Elaboración propia

Sera evaluada a través del modelo de evaluación de Likert, la cual se define como una herramienta para poder cuantificar que haciendo un contraste con las preguntas dicotómicas con respuesta sí/no, nos permite medir actitudes y conocer el nivel de conformidad del usuario con cualquier afirmación que le planteemos. La escala de medición aplicada será:

- TD: Total desacuerdo

- D: Desacuerdo
- N: Neutro
- A: Acuerdo
- TA: Totalmente de acuerdo

Aplicarla resultaría útil en escenarios en los que queremos que la persona matice su opinión. En este caso, las categorías de respuesta nos servirán para capturar la intensidad de las opiniones del usuario hacia dicha afirmación.

2.10 ANÁLISIS COMPARATIVO

- **Variable dependiente:**
 - Participación del usuario
- **Indicadores:**
 - Participación en el uso de herramientas de seguridad de la información
 - Participación en la seguridad de los sistemas de información
 - Participación en la identificación del riesgo en TI
 - Participación en proyectos tecnológicos
 - Participación en la ejecución de pruebas de control
- **Variable dependiente:**
 - Planificación de los sistemas de información
- **Indicadores:**
 - Control al sistema de información

- Control de recursos de infraestructura tecnológica
- Control de recursos de software
- Metodología de implementación
- Estrategia de sistemas de información
- **Variable independiente:**
 - Desempeño de mecanismos de seguridad de la información
- **Indicadores:**
 - Control y procedimientos de acceso al sistema de información
 - Segregación de funciones en el sistema de información
 - Políticas de seguridad y acceso al sistema

2.11 ANÁLISIS CRÍTICO

Se analizarán las variables en una escenario pre prueba, es decir en un estado natural donde se estudiarán y medirá su correlación.

Luego se aplicarán cambios en los mecanismos de seguridad de la información y se volverá a analizar un escenario pos prueba donde se analizará su correlación y se respectiva variación.

Concluyendo con un análisis de la relación entre las 3 variables a través de mediciones de sus indicadores.

CAPÍTULO III

MARCO REFERENCIAL

En el presente capítulo se representan los datos generales de la unidad minera Pucamarca perteneciente a Minsur SA (Minsur, 2018), su reseña histórica, su filosofía empresarial, sus principales minerales de producción asimismo todo lo que implica su información como empresa en general.

3.1 RESEÑA HISTÓRICA

El inicio de la empresa radica en el siglo XX, cuando Lampa Mining Company operaba en la región Puno. Luego de esta compañía varias décadas después en 1966, se establece Minsur Sociedad Limitada, dependencia peruana de la minera Minsur Partnership Limited de Bahamas, la cual es adquirida en el año 1977 por el Grupo Breca para ser convertida en Minsur S.A., una organización de capitales 100% peruanos. Luego de la adquisición y por unos años más, el producto estrella de aquel entonces en la UM San Rafael era el cobre. Luego de 1992 el estaño pasó a ser el insuperable metal producido en dicha unidad, sin embargo, años más tarde también explotaría cobre.

Desde el año 2012 operan en la provincia de Palca, Tacna. La UM Pucamarca, ubicada en la frontera con Chile, tiene un cash cost promedio de 4.4 dólares por tonelada tratada (USD/tt). Mediante los procesos de chancado y lixiviación, se reduce el tamaño del mineral que proviene de la mina y se separa el metal de la roca. Luego, se funde en un horno eléctrico para obtener barras de doré de 60 % a 70 % de pureza.

3.2 MISIÓN Y VISIÓN

La misión y visión de la empresa, así como sus valores, reflejan su compromiso con una gestión responsable, que impulsa la sostenibilidad en todos los niveles de la organización: desde el proceso de toma de decisiones hasta su implementación.

- Misión: Generar valor transformando recursos minerales de manera sostenible.
- Visión: Desarrollar y operar activos mineros de clase mundial, siendo un referente en términos de seguridad, eficiencia operacional, responsabilidad socioambiental y desarrollo de personas.

3.3 VALORES

Figura 28



Figura 28. Los Valores de la empresa. Reimpreso de Memoria anual 2018. Copyright 2018 por Minsur.

En la figura 28 se presentan los seis valores con los que se tutelan los colaboradores de la empresa Minsur, los cuales son excelencia, compromiso,

integridad, responsabilidad, confianza y seguridad.

3.4 DESEMPEÑO OPERATIVO

Durante el 2018, la producción de oro de Pucamarca se incrementó en 6% en comparación con el año anterior. De acuerdo con los objetivos planteados, se logró sostener la producción en 21,000 tpd. Como consecuencia, la producción de este periodo superó las 103,000 onzas de oro, en línea con el plan de minado del yacimiento.

Pucamarca se mantiene como una de las minas de oro de menor costo en el mundo. El cash cost por tonelada tratada en el 2018 alcanzó USD 4.4, incrementando 3% respecto al 2017. Este incremento de costos se debe principalmente a pruebas realizadas para tratar el mineral de la zona de Morrenas, que se empezará a extraer de manera parcial a partir del 2019, y que está dentro de lo previsto en el plan de minado.

Es importante recalcar que se concluyeron los estudios y se confirmó la viabilidad del uso del río Azufre para asegurar un nuevo suministro de agua para la operación. La construcción de la planta de tratamiento de agua se encuentra en curso y se espera que inicie operaciones en el 2019 y abastezca a la UM. Por otro lado, continúan el programa de exploraciones “Pucamarca Regional”, orientado al esclarecimiento de potenciales objetivos de exploración para la prolongación de la vida de la mina. Durante el 2018, las inversiones estuvieron enfocadas principalmente en la construcción del PAD 3B, botadero,

desmontera, planta de agua y en el mantenimiento de nuestros equipos.

Figura 29

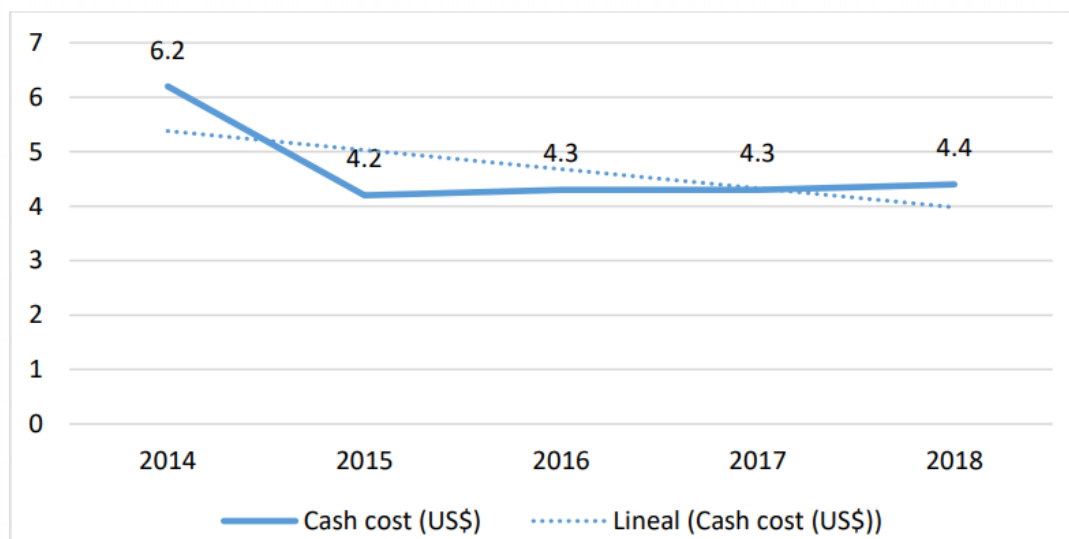


Figura 29. Cash cost por tonelada tratada. Reimpreso de Memoria anual 2018. Copyright 2018 por Minsur.

Tabla 16
Indicadores de producción

Categoría	Indicador	Unidad	2018	2017	2016
Mina	Mineral tratado	t	8'242,116	7'715,582	7'692,322
	Ley mineral extraído	g/t	0.6	0.5	0,5
PAD	Mineral colocado en PAD	t	8'219,641	7'801,777	7'692,322
	Ley mineral colocado en PAD	g/t	0.6	0.5	0,5
Planta	Onzas oro producidas	oz	103,538	100,01	105,659
	Recuperación histórica	%	74.64	75.84	74.88
	Utilización planta	%	98.01	98.01	98.01
Unidad Minera	Costo por tonelada tratada	USD/tt	4.42	4.33	4.30

Nota: Adaptado de Memoria anual 2018, Minsur.

Tabla 17
Reservas de la UM Pucamarca

Clase	Cut Off Au (g/t)	Mt	Au g/t	Contenido Au Koz
Probado	Variable	14,6	0,52	243,4
Probable	Variable	19,3	0,5	308,1
Total reservas		33,9	0,51	551,5

Nota: Adaptado de Memoria anual 2018, Minsur.

Notas:

- Los recursos minerales incluyen a las reservas minerales.
- Los recursos y reservas están restringidos a pits shell optimizados correspondientes a tres zonas: Checocollo, Morrenas y Caldero.
- Para la estimación de recursos minerales aplica el precio de USD 1,400/oz para el Au.
- En Morrenas, el límite de estimación de recursos y reservas del lado de la frontera Perú-Chile se ha reconsiderado en 30 m (anterior fue de 100 m) en concordancia a aspectos legales vigentes.
- Para la estimación de reservas se usó el precio de USD 1,200/oz para el Au.
- Los recursos y reservas minerales han sido auditados por la empresa externa e independiente Amec Foster Wheeler Perú S.A.

3.5 GESTIÓN SOCIAL

La misión de la empresa se centra en la obtención de valor sostenible a través de la transformación de recursos minerales, para ello, la empresa maneja una estrategia de gestión social que se apoya en los siguientes tres pilares: Relacionamiento efectivo, Inversión Social y Monitoreo de riesgos sociales.

Relacionamiento con comunidades

La gestión con las comunidades en las zonas de influencia se centra en la creación de vínculos de largo plazo, desde las etapas tempranas de vida de cada mina. Para ello, se usan distintos mecanismos de participación y comunicación, cuya naturaleza varía según la unidad minera, y diversos factores, como el conjunto de personas, sus costumbres, los riesgos particulares en la zona.

En Minsur reciben con atención la opinión de sus grupos de interés para la constante mejora de su desempeño y atienden sus inquietudes de manera armónica. Las personas de la comunidad pueden informar sus quejas, reclamos o sugerencias a través de diversos medios, según la unidad o proyecto tales como Oficinas Permanentes de información, visitas a campo, formatos de quejas y reclamos, entre otros.

La inversión social

En Minsur, contribuyen al desarrollo de las poblaciones vecinas mediante la mejora de las capacidades locales, desde un escenario de género, inclusión social e interculturalidad. Por eso se tienen en cuenta las necesidades

puntuales de cada población con que se relaciona, y la promoción de un enfoque de multiactor (estado-comunidad-empresa). Existen cuatro líneas de inversión en las que se basan sus iniciativas de desarrollo local.

Figura 30

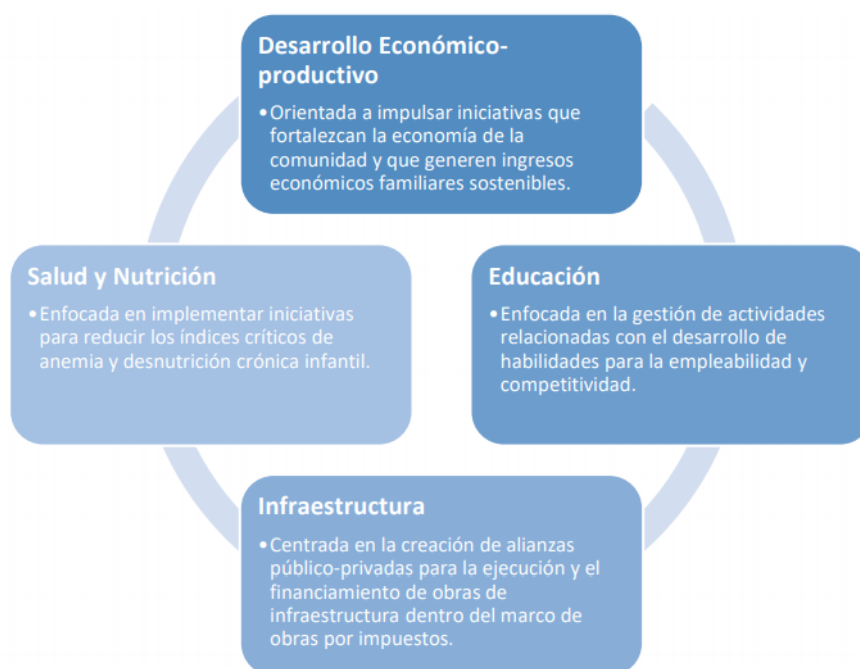


Figura 30. Programas de desarrollo social. Reimpreso de Memoria anual 2018. Copyright 2018 por Minsur

En Pucamarca se continuó con proyectos productivos, como el de fortalecimiento de las capacidades de crianza y comercialización de animales menores en la C. C. de Vilavilani, y el fortalecimiento de capacidades en cultivos de pan en la C. C. de Palca. También se construyó un reservorio de agua para riego de 5,200 m³ y 3 invernaderos en las instituciones educativas de las comunidades de Vilavilani y Palca.

Además, se implementó material educativo y de seguridad en las instituciones educativas de Palca y Vilavilani, y se mejoró la loza de patio de la I. E. de Palca. También se dictaron capacitaciones en temas relacionados con la

nutrición infantil.

3.6 GESTIÓN AMBIENTAL

En Minsur desarrollan negocios con un énfasis permanente en el cuidado del medio ambiente y la reducción de sus impactos ambientales. Su marco de políticas corporativas integra principios transversales de sostenibilidad para garantizar que se ejecute una debida diligencia en todos los procesos y operaciones de la compañía. Las operaciones de Pirapora, Pisco, Pucamarca y San Rafael cuentan con la certificación ISO 14001, una certificación internacional que proporciona a las organizaciones un marco para proteger el medio ambiente. Si bien la UM Pitinga aún no cuenta con esa certificación, todas sus operaciones y proyectos cuentan con el mismo Sistema Gestión Ambiental (SGA), diseñado con base en la ISO 14001.

El SGA rige bajo la Política de Sostenibilidad y se ejecuta de acuerdo con el Manual Corporativo SGA; que cuenta con estándares de gestión y de operación en materia ambiental. Estos son adoptados por todo el personal involucrado (propio y contratista) en los procesos de operación y soporte, y permiten asegurar el cumplimiento de los requisitos legales en todas las etapas mineras.

Es importante señalar que, en línea con el principio del ICMM que busca la mejora continua del desempeño ambiental de sus miembros. En el 2018 se realizó la revisión de sus estándares de gestión y de operación en materia ambiental y los resultados serán aprobados en el 2019 para su

implementación.

El SGA tiene 5 pilares fundamentales que están alineados con la misión y la visión de Minsur.

Figura 31



Figura 31. Pilares del SGA. Reimpreso de Memoria anual 2018. Copyright 2018 por Minsur.

En Minsur se evalúan los impactos ambientales durante todas las fases de la vida de la mina, empezando por la fase de exploraciones hasta las actividades posteriores a su cierre. Para ello, cuentan con las siguientes herramientas:

Figura 32

Auditorías internas	Indicadores de desempeño ambiental	Monitoreo ambiental	Fiscalización ambiental
<ul style="list-style-type: none">• Se realizan para determinar el grado de conformidad de las operaciones con el Sistema de Gestión Ambiental y los requisitos legales aplicables, así como para validar la eficacia del SGA. En caso de detectar un desempeño por debajo del estándar, el superintendente de Medio Ambiente de la unidad o proyecto implementará las acciones correctivas solicitadas en el informe final de auditoría y, posteriormente, preparará un informe en el que reportará el resultado de la ejecución de estas acciones. También se realizan auditorías cruzadas.	<ul style="list-style-type: none">• De manera mensual, los superintendentes de Medio Ambiente registran y evalúan los indicadores de desempeño ambiental (IDA). A través de ellos, se miden y monitorean los impactos ambientales y los potenciales riesgos. Estos indicadores son reportados al gerente de Medio Ambiente en reuniones mensuales para identificar y definir los puntos de mejora a ser implementados.	<ul style="list-style-type: none">• En las áreas de influencia de las unidades y proyectos se han establecido puntos de monitoreo para la evaluación continua de ruido y de la calidad de aire, suelo y agua, autorizados por las autoridades competentes. De manera complementaria, en algunas de las unidades se han implementado monitoreos ambientales participativos en los que se involucra a las comunidades de influencia directa.	<ul style="list-style-type: none">• Nuestro desempeño ambiental es fiscalizado de manera periódica por el Organismo de Evaluación y Fiscalización Ambiental (OEFA) en el Perú; el Instituto de Proteção Ambiental do Amazonas (IPAAM) en la región Amazonas, y la Companhia Ambiental do Estado de São Paulo (CETESB) en la región de Sao Paulo, en Brasil. El objetivo es corroborar el cumplimiento de las normas legales, los instrumentos de gestión ambiental, los procesos de obtención de permisos, los mandatos o disposiciones emitidas por los órganos competentes, así como otras fuentes de obligaciones ambientales fiscalizables.

Figura 32. Herramientas de control de Medio Ambiente. Reimpreso de Memoria anual 2018. Copyright 2018 por Minsur.

3.7 GESTIÓN DEL AGUA

En todas las actividades mineras buscan reducir la cantidad de agua con el principio de aplicar una gestión eficiente de este recurso. Esto está contemplado desde el diseño de la infraestructura de todas las unidades, en sus operaciones, a través de la reutilización y reciclaje de gran parte del agua consumida, así como en las diferentes iniciativas de ahorro desarrolladas en cada una de ellas.

Sus equipos de medio ambiente controlan la calidad y cantidad de agua de manera periódica en cumplimiento con los requisitos legales y sus propios estándares de operación. De manera complementaria, y como muestra de transparencia, programan monitoreos que se realizan con participación de miembros de las comunidades locales. Cabe resaltar que este año no tuvieron fuentes significativas afectadas por extracción.

Tabla 18
Extracción de agua por fuente (miles de m³/año)

Fuente	UM San Rafael	UM Pucamarca	PFR Pisco	UM Pitinga	PFR Pirapora
Aguas superficiales	1,993	1	0	8,918.1	0
Aguas subterráneas	7,627	369	247,829	0	79.62
Agua de lluvia recogida y almacenada directamente por la organización	0	0	0	0	0
Total	9,561	370	247,829	8,918.1	79.62

Nota: Adaptado de Memoria Anual 2018, Minsur.

3.8 GESTIÓN DE RESIDUOS

Todas sus unidades cuentan con un programa de recojo de los residuos

sólidos de la red de depósitos, a cargo de un contratista especializado. El material es segregado y recirculado al proceso, mientras que otros, como la madera, es dispuesta por una EPS certificada y autorizada. Para el recojo, el transporte de los residuos sólidos y el vertimiento en rellenos sanitarios autorizados o plantas de tratamiento, se cuenta con una empresa prestadora de servicios certificada por Digesa. Además, se sensibiliza de manera permanente a todo el personal respecto a la generación y disposición adecuada de los residuos sólidos generados durante las operaciones productivas, de mantenimiento, logísticas, entre otras.

Tabla 19

Residuos peligrosos y no peligrosos por tipo de eliminación (t/año)

Tipo de eliminación	UM San Rafael	UM Pucamarca	PFR Pisco	UM Pitinga	PFR Pirapora
Residuos peligrosos					
Reciclaje	94	55	0	69	2
Relleno de seguridad fuera de la unidad	346	41	0	0	0
Incineración	0	0	0	51	5.96
Sub total	445	95	30.81	120	7.97
Residuos no peligrosos					
Reutilización	122	168	0	0	0.32
Reciclaje	1351	0	0	42	5.53
Compostaje	9	54	0	0	0
Incineración (quema de masa)	0	0	0	139	0
Relleno Sanitario fuera de la unidad	135	156	0	90	53.84
Relleno Sanitario dispuesto en la unidad	369	0	0	17	0
Sub total	1986	378	260.7	288	59.59
Total	2431	473	291.51	408	67.65

Nota: Adaptado de Memoria Anual 2018, Minsur.

3.9 GESTIÓN DE EMISIONES

Minsur considera muy importante controlar las emisiones que generan sus actividades mineras para no alterar la calidad del aire, proteger el medio ambiente y cuidar la salud del personal y de las comunidades vecinas. Gracias a las medidas de control y monitoreo, los niveles de las emisiones cumplen con los límites máximos permisibles establecidos por la ley. Estos incluyen el monitoreo de ruido, polvo y gases. Como resultado del compromiso de la empresa con la reducción de emisiones de gases de efecto invernadero y prevención del calentamiento global. En el 2018 se realizó por primera vez la medición de nuestra huella de carbono con los estándares ISO 14064-1 y GHG Protocol. Esta acción se repitió a inicios de 2019 con el fin de obtener resultados comparativos a la línea base. Cabe señalar que las mediciones fueron realizadas por una consultora y que los resultados aún no han sido auditados, pero se tiene planificado realizarlo en el corto plazo.

Tabla 20
Variación de las emisiones por unidad

Unidad	Variación	
	2017-2018	Análisis
Oficina Lima	139.3%	La principal fuente de emisión, viajes en avión, ha aumentado de manera considerable (x3).
UM Pucamarca	6.7%	Se registra un mayor consumo de combustible por maquinarias móviles. Además, hay un mayor consumo de electricidad (+8%)
PFR Pisco	1.4%	Si bien hay una reducción de emisiones por un menor uso de la Central Térmica, se diluye este efecto por un mayor consumo de combustible de equipos estacionarios y de carbón como agente reductor
UM San Rafael	-6.3%	Se reporta un menor consumo de combustible por maquinarias móviles de contratistas, y adicionalmente, hay un menor consumo de electricidad (-3%)

UM Pitinga	13.1%	Se reportó un considerable aumento en el consumo de combustible de generadores eléctricos, debido al periodo de estiaje que disminuyó la generación hidroeléctrica
PFR Pirapora	11.4%	Aumenta considerablemente el uso de carbón como agente reductor (+37%)

Nota: Adaptado de Memoria Anual 2018, Minsur.

3.10 GESTIÓN DE ENERGÍA

Cada día la empresa reafirma su compromiso de responsabilidad en la lucha contra el cambio climático. Este compromiso se vincula con la mejora continua de sus estándares ambientales, la promoción de conciencia sobre la protección ambiental y el monitoreo constante y preventivo de sus operaciones. Con el objetivo de hacer más eficiente el consumo energético y reducir la generación de emisiones al medio ambiente. En Minsur miden y registran los niveles de consumo de este recurso en todas las unidades y proyectos.

Tabla 21
Consumo total de energía (GJ)

Consumo	UM San Rafael	UM Pucamarca	PFR Pisco	UM Pitinga	PFR Pirapora
Consumo total de combustibles	262651	239812.33	573.592	137301	0
Consumo total de electricidad	147830	73133.17	90197.12	550980	139058.05
Consumo total de energía	410481	312945.5	95578.12	688281	139058.05

Nota: Adaptado de Memoria Anual 2018, Minsur.

3.11 DIAGNÓSTICO SECTORIAL

Para determinar un mejor entendimiento del poder competitivo de la organización en su respectivo sector, y formular estrategias que aprovechen las oportunidades del propio mercado además de defenderse de las amenazas existentes se realizará el modelo de análisis de las 5 fuerzas de Porter.

Figura 33



Figura 33. Las 5 fuerzas de Porter. Copyright www.5fuerzasdeporter.com

3.11.1 Poder de negociación de los proveedores

El grupo de organizaciones que proporcionan productos y servicios para efectuar las actividades centrales de exploraciones, chancado, beneficio y

comercialización de los concentrados de minera son los distintos proveedores de la UM Pucamarca, los más importantes entre ellos son los que abastecen equipos de maquinaria pesada, insumos, como herramientas de perforación y molienda, combustibles, explosivos y energía, respectivamente. En el año 2006 y 2012, se dispara la demanda y se da el crecimiento de precios de los minerales, los precios de servicios y suministros. Así mismo, los tiempos de entrega ascendieron entre 1,5 a 4,0 veces. Este prospero escenario llevo a otorgar a varios proveedores cierto nivel de dominio en las negociaciones; sin, no obstante, luego del año el 2013 y manteniendo la espera nuevamente a la era del incremento de precios de los metales, el poder de negociación regresó a la empresa minera.

3.11.2 Poder de negociación de los clientes

Pucamarca Minsur proporciona al mercado un beneficio básico llamado concentrado, el cual requiere de otros procesos especializados como fundición y refinación con el objeto de obtener metales en barras, láminas y otras presentaciones. Estas barras tienen un grado de pureza solicitado; por lo tanto, los clientes importantes de la organización son empresas comercializadoras de concentrados. Acorde al panorama de la demanda del mercado, los clientes establecen los términos de los acuerdos comerciales, los cuales son los plazos de entregas de la producción en toneladas métricas húmedas por lotes mensuales, porcentaje de humedad permitido, precio inicial, márgenes de los contenidos pagables y máximo límite de polución, esto somete a la empresa

minera a efectuar cambios en su plan de producción según el contrato vigente. El poder de negociación por lo general está en manos del cliente, excepto en el escenario cuando se disponga una cantidad alta de producción de concentrado que da la posibilidad de obtener superiores condiciones por volumen de producto.

3.11.3 Amenaza de nuevos competidores

Todas las precedentes de requerimientos ambientales, sociales, regulatorios, financieros y periodo de maduración son las dificultades para el ingreso de nuevos competidores en el sector de minería, desde el inicio en la exploración hasta el inicio en operación comercial que demanda un proyecto minero. Justamente son los factores burocráticos, más la alta cantidad de permisos, generan que algunos competidores dimitan de ingresar en el segmento de minería. En el país existen grandes proyectos de minería diferidos por la coyuntura, los cuales se encuentran aplazados. En el horizonte analizado debido a la competencia casi perfecta, la mayoría de ellos ingresaran al mercado; no obstante, podrán realizarlo siempre y cuando sean técnica y económicamente sustentables. La viabilidad de un proyecto de minería está en función de la calidad de minerales y la cantidad que tiene el depósito; de la bondad de sus indicadores fruto de un flujo de caja financiero y económico, visionado a lo largo de la vida útil de la cantera, con base en una manufactura planificada, precios de venta estimados, la recuperación metalúrgica determinada, y otros factores operacionales propios del negocio.

3.11.4 Amenaza de productos o servicios sustitutos

Actualmente, no es posible encontrar sustitutos para los minerales que la UM Pucamarca produce, como lo son el oro y plata. Podemos decir esto basándonos en el reporte a continuación: Según el reporte Mining&Metals World Economic Forum (2015) in a Sustainable World 2050, indica que la minería no va desaparecer. Continuará la extracción primaria, pero es improbable con su volumen no vaya en paralelo con el crecimiento PBI. Esto quiere decir que la influencia por realizar los efectos de escala y eficiencia de costos, permanecerá en un futuro previsible. Y que la demanda por costos efectivos coexistirá en paralelo con las operaciones de responsabilidad social y medioambiental, dando cabida a otras formas de asociación y modelos de operación, por lo cual decimos que no existe amenaza de productos sustitutos por ahora; sino por el contrario, hay una alta tendencia de que los inversionistas aumenten la compra de oro y plata, para acumular metales preciosos como reservas durante las crisis y la volatilidad de las economías, que se desarrollan repetitivamente en el acontecer mundial.

3.11.5 Rivalidad entre los competidores existentes

No se da rivalidad entre competidores en lo que respecta a la demanda, precios y calidad del mineral concentrado, esto a razón de que los minerales son commodities. Viéndolo desde un enfoque sectorial, afirmamos que existe

rivalidad por obtener la mejor eficiencia operativa de la mano con el menor costo operativo de producción y mercantización, además de tener mejor calidad y mayor cantidad de existencias de mineral, como activo económico más importante.

CAPÍTULO IV

RESULTADOS

En este capítulo se presentarán los mecanismos de seguridad de la información implementados, así como la información recolectada en dos escenarios pre y post prueba, dicha información será procesada, analizada e interpretada para las variables del estudio y así finalmente poder validar las hipótesis de la investigación.

4.1 MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS SEGÚN LAS VARIABLES, INDICADORES Y PREGUNTAS

Producto del análisis de los problemas evaluados en combinación con la bibliografía estudiada se desarrollaron herramientas según la necesidad de la empresa, las cuales sirvieron para apoyar el desempeño de las variables, indicadores e ítems desarrollados.

Cabe señalar que estas herramientas se desarrollaron exclusivamente para el post prueba de la investigación a fin de estudiar el contraste de puntuación de los indicadores.

Tabla 22
Variables – Indicadores – Ítems - Mecanismos

VARIABLE	INDICADOR	ITEM EN CUESTIONARIO	ACCION	MECANISMO
Participación del usuario	Participación en el uso de herramientas de SI de su empresa	Participa en capacitaciones acerca del uso de las herramientas de seguridad informática de su área	Capacitar a los usuarios finales en el uso de las herramientas de seguridad informática	REGISTRO DE CAPACITACIONES
	Participación en la seguridad de los SI	Tienen en cuenta su opinión para el diseño de los sistemas de SI de su empresa	Hacer partícipes a los usuarios finales en la implementación de herramientas de SI	REGISTRO DE CAPACITACIONES
	Participación en la identificación del riesgo en TI	Participa identificando riesgos en los sistemas informáticos que usa	Identificar los riesgos de IT según los procesos a realizar	IPERC
	Part. en proyectos tecnológicos	Tienen en cuenta su opinión para la automatización en proyectos tecnológicos de la empresa	Hacer partícipes a los usuarios finales en la automatización de procesos	FORMATO DE ESPECIFICACION DE REQUERIMIENTO
	Part. en la ejecución de pruebas de control	Participa en pruebas/certificación de los sistemas informáticos a implementar	Hacer partícipes a los usuarios al final testing de software	ENTREVISTAS
Planificación de los SI	Control al SI	En la planificación de proyectos, hay supervisión los puntos correspondientes a TIC	Hacer partícipes a las áreas durante la fase de planificación	FORMATO DE ESPECIFICACION DE REQUERIMIENTO
	Control de recursos de infraestructura tecnológica	Cree que la empresa planifica y ejerce control de los recursos de infraestructura tecnológica	Gestionar los productos de hardware de la empresa	INVENTARIO HARDWARE
	Control de recursos de software	Cree que la empresa planifica y ejerce control de los recursos de software	Gestionar los productos de software de la empresa	INVENTARIO SOFTWARE
	Metodología de implementación	Considera que hay una metodología para la implementación de sistemas de información	Seguir una metodología de implementación de SI	SEGÚN EL PROVEEDOR
	Estrategia de SI	Cree que los SI son producto del análisis de proyectos tecnológicos a fin de apoyar las estrategias de la empresa	Programar reuniones con las áreas usuarias para evaluar los SI	FORMATO DE ESPECIFICACION DE REQUERIMIENTO
Desempeño de mecanismos de seguridad de la información	Control y procedimientos de acceso al SI	Se encuentra satisfecho con los SI de su área, percibe un adecuado control	Evaluar opinión de sistemas de las áreas	ENTREVISTAS
	Segregación de funciones en el SI	Según su área considera alta la concentración de funciones de los SI de su área	Analizar los procesos del área usuario buscando procesos a automatizar	IPERC
	Políticas de seguridad y acceso al sistema	Existen políticas y normas implementadas que mejoran el desempeño del sistema y de los usuarios	Desarrollar un marco de seguridad de la información	*REGISTRO DE RESTAURACION DE BACKUPS *FILTRADO MAC

Nota: Elaboración propia

Registro de capacitaciones

Desarrollado como herramienta de control de participación de usuarios y áreas a las distintas actividades que buscan promover su inclusión en los procesos de diseño y uso de los sistemas de información

Figura 34










MINSUR		FORMATO REGISTRO DE ASISTENCIA DE ACTIVIDADES FORMATIVAS		Código:	UM-PU-PG-019-F-003
				Versión:	0
				Fecha de aprobación:	28/08/2014
				Páginas:	1
Tema / Actividad		Capacitación Itepum y susso			
Area o Equipo		Sistema			
Hora de inicio		08:00 pm		Hora de Término: 08:40 pm	
Fecha		10/02/19			
Lugar		Sala WICP / Timuna			
Facilitador/Responsable		Tina Alvarado Espinoza		Firma: 	
Nº	Código Personal/DNI	Apellidos y Nombres	Área / Empresa	Firma	
1	00773994	Eberle Atencio Cl.	RR-HH / Pegasus		
2	20507225	Alfonso Rueda	Pegasus		
3	41814131	ESPINOZA GUILERMO ANAH	RR-HH / Pegasus		
4	40695506	Flamini Drenage, Edile	RR-HH / Pegasus		
5	40409263	Cauma Wianaca Lucas	RR-HH / Pegasus		
6	40102697	Castro Celque David	RR-HH / Pegasus		
7	02514763	Villabaz Jose	RR-HH / Pegasus		
8	46284470	Gilmer Espinoza P.	RR-HH / Pegasus		
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					

Figura 34. Formato de registro de asistencia. Elaboración propia

Formato de especificación de requerimiento

Es el mecanismo donde se obtiene la descripción completa del comportamiento del futuro sistema de información. Aquí se registran las necesidades del negocio y se definen los requerimientos que debe cumplir el producto o sistema. Por tanto, es el medio de comunicación entre los usuarios y desarrolladores.

Tabla 23

Formato de especificación de requerimiento

RF - <id>	<Nombre descriptivo>	
Versión	<Número de versión actual> (<Fecha de versión actual>)	
Autor	<Autor de versión actual> (<Compañía del autor>)	
Propósito	<Propósito del requerimiento>	
Descripción	El sistema debe comportarse como se describe en la siguiente secuencia de interacciones cuando <evento disparador>	
Alcance Y Nivel	<Que sistema es considerado caja negra en la perspectiva de diseño>	
Precondición	<Lo que se espera del entorno para la realización del requerimiento>	
Condición de Éxito	<Estado del entorno que indica que se realizó con éxito>	
Condición de Fracaso	<Estado del entorno cuando el requerimiento es abortado o falla>	
Actores	<Primario> {<Secundarios>}	
Evento Disparador	<Evento disparador o trigger>	
Secuencia Norma	Paso	Acción
	n	{ el { <actor>. Sistema} <acción
	n.1	{ el { <actor>. Sistema} <acción ejecutada por actor/sistema>, Pasos descritos en <caso de uso (RF-x)> es

Postcondición	<Postcondición del caso de uso>	
Excepciones Y Extensiones	Paso	Acción
	p	if <condición de excepción>, { el {
INFORMACIÓN RELACIONADA		
Prioridad	<grado de prioridad del requerimiento>	
Frecuencia	Este caso de uso se espera ser ejecutado <número de veces> número de veces/ <unidad de tiempo>	
Desempeño	Paso	Acción
	q	m segundos

Canales hacia los Actores	<Archivos, interactivo, base de datos, etc>	
Características Abiertas	<Lista de características que pueden afectar las decisiones sobre el caso de uso>	
Superiores	<Lista de requerimientos que incluyen este requerimiento>	
Comentarios	<comentarios adicionales acerca del requerimiento>	

Nota: Elaboración propia

Entrevistas

Mecanismo que da la posibilidad de plasmar conversaciones, opiniones y criterios siguiendo una estructura definida por nosotros, a través de preguntas para el usuario. Usamos este mecanismo para ver analizar la opinión el usuario acerca de sus sistemas y su implementación cada cierto periodo de tiempo.

Figura 37

ENTREVISTA : ESTADO ACTUAL DE LAS TIC EN PUCAMARCA	
	Lugar: Unidad Minera Pucamarca Minsur Fecha:
1. ¿Usted cree que la información relacionada con los sistemas de información de su área, es correcta y nunca ha sido modificada?	En su momento de perdición ultimamente, pero a lo largo de los años se reparten bastante
2. ¿Usted cree que la información relacionada con los sistemas de información de su área, es confidencial y solo puede acceder a ella personal autorizado?	Libro oculto en modo lectura, todos pueden solo leer solo más área, TIC y generación lo cual se debe cuidar bien.
3. ¿Usted cree que la información relacionada con los sistemas de información de su área, es altamente disponible?	Si, no siempre, se han producido caída del servicio por distintos motivos (proceder, redudanza i negligencias)
4. ¿Usted cree que los usuarios de las distintas áreas se encuentran al tanto de sus sistemas, aplicaciones y equipos de automatización y su correcto uso?	No totalmente, existen varios sistemas por los que se paga y no se usan
5. ¿Usted cree que existe una buena proyección acerca de los recursos de TIC en la empresa?	Si hay una buena inversión y proyección pero se deben dirigir correctamente a los requeridos de la empresa
6. ¿Se encuentra al tanto de los procedimientos, políticas y tareas que abarca el área de TIC de la empresa?	No,
7. ¿Usted cree que hay adecuado control de la información en la empresa?	No, se han reportado cuestion de perdida de la información



Victor Rivas

 Analista de Negocio

Figura 37. Entrevista desarrollada. Elaboración propia.

Inventario de Hardware

Mecanismo desarrollado para llevar un control claro y preciso acerca de los elementos de hardware de la empresa según los criterios o campos clave del área.

Figura 38

Nº	Usuario	Area	Tipo	Ubicación	Situación	Hostname	Marca	Modelo	Tipo / Product. ID	Serie	Procesador	Memoria	Disco	Tarjeta de Red MAC	Tarjeta Inalambrica MAC	SO	MS OFFICE	Contrato	Fecha de Inicio
1	*****	Seguridad	Laptop	Pucamarca	Asignado	PUCSEGUARDIAHP	HP	Compaq (CIV)9072120		*****	Intel(R) Core(TM) i7-2630M	232 GB	232 GB	00-24-81-3F-00-21-68-98-18		Windows 7 Estándar	Office 2007		
2	*****	Seguridad	Laptop	Pucamarca	Asignado	PUCICAMPUSLLENDOVO	HP	Thinkpad T420U-A11X80		*****	Intel(R) Core(TM) i5-3320M	215 GB	215 GB	50-7B-9D-A4-10-02-85-36-2F		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
3	*****	Mina	Laptop	Pucamarca	Asignado	PUCRINIEDAELLENDOVO	HP	Thinkpad T420U-A11X80		*****	Intel(R) Core(TM) i5-3320M	215 GB	215 GB	50-7B-9D-A4-10-02-85-36-2F		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
4	*****	Planta	Laptop	Pucamarca	Asignado	PUCBSAMENELLENDOVO	HP	Thinkpad T420U-A11X80		*****	Intel(R) Core(TM) i5-3320M	215 GB	215 GB	50-7B-9D-A4-10-02-85-36-2F		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
5	*****	Planta	Laptop	Pucamarca	Asignado	PUCCEPEORIELLENDOVO	HP	Thinkpad T420U-A11X80		*****	Intel(R) Core(TM) i5-3320M	215 GB	215 GB	50-7B-9D-A4-10-02-85-36-2F		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
6	*****	Planta	Laptop	Pucamarca	Asignado	PUCRSEGUARDIAHP	HP	Thinkpad T420U-A11X80		*****	Intel(R) Core(TM) i5-3320M	215 GB	215 GB	50-7B-9D-A4-10-02-85-36-2F		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
7	*****	Mantenimiento	Laptop	Pucamarca	Asignado	PUCIARRANASLLENDOVO	HP	Thinkpad T420FA0N(G)00		*****	Intel(R) Core(TM) i5-3320M	512 GB	512 GB	08-5B-76-5C-E4-A7-A0-83-70		Windows 7 Hogar	Microsoft 2010	Anexo 02/08/2016	02/08/2016
8	*****	RRHH	Laptop	Pucamarca	Asignado	PUCIZAGABARALLENDOVO	HP	Thinkpad T4620FA-40N(G)00		*****	Intel(R) Core(TM) i5-3320M	512 GB	512 GB	59-76-5C-BE-84-60-C7-53-F1		Windows 7 Hogar	Microsoft 2010	Anexo 02/08/2016	02/08/2016
9	*****	Seguridad	Laptop	Pucamarca	Asignado	PUCIAREDESIELLENDOVO	HP	Thinkpad T420U-A11X80		*****	Intel(R) Core(TM) i5-3320M	215 GB	215 GB	50-7B-9D-A4-10-02-85-36-2F		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
10	*****	Sistemas	Laptop	Pucamarca	Asignado	PUCIAREDESIELLENDOVO	HP	Thinkpad X120M1-A19V00		*****	Intel(R) Core(TM) i5-3320M	300 GB	300 GB	54-EE-75-8E-10-02-85-AF-FF		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
11	*****	Costos y Pre-laptop	Laptop	Pucamarca	Asignado	PUCIAREDESIELLENDOVO	HP	Thinkpad X120M1-A19V00		*****	Intel(R) Core(TM) i5-3320M	300 GB	300 GB	54-EE-75-8E-10-02-85-AF-FF		Windows 7	Microsoft 2010	Anexo 01/07/2016	01/07/2016
12	*****	Planta	Laptop	Pucamarca	Asignado	PUCRCONSUMO DELL	HP	Latitude E741199421742		*****	Intel(R) Core(TM) i5-3320M	250 GB	250 GB	34-6B-D7-15-48-51-B7-20-CC		Windows 7	Microsoft 2010	Anexo 01/11/2014	01/11/2014
13	*****	Planta	Laptop	Pucamarca	Asignado	PUCRCONSUMO DELL	HP	Latitude E741199421742		*****	Intel(R) Core(TM) i5-3320M	250 GB	250 GB	34-6B-D7-15-48-51-B7-20-CC		Windows 7	Microsoft 2010	Anexo 01/11/2014	01/11/2014
14	*****	Mantenimiento	Laptop	Pucamarca	Asignado	PUCIAREDESIELLENDOVO	HP	Latitude E741199421742		*****	Intel(R) Core(TM) i5-3320M	250 GB	250 GB	34-6B-D7-15-48-51-B7-20-CC		Windows 7	Microsoft 2010	Anexo 01/11/2014	01/11/2014
15	*****	Mantenimiento	Laptop	Pucamarca	Asignado	PUCIAREDESIELLENDOVO	HP	Latitude E741199421742		*****	Intel(R) Core(TM) i5-3320M	250 GB	250 GB	34-6B-D7-15-48-51-B7-20-CC		Windows 7	Microsoft 2010	Anexo 01/11/2014	01/11/2014
16	*****	RRHH	Laptop	Pucamarca	Asignado	PUCIAREDESIELLENDOVO	HP	Latitude E741199421742		*****	Intel(R) Core(TM) i5-3320M	250 GB	250 GB	34-6B-D7-15-48-51-B7-20-CC		Windows 7	Microsoft 2010	Anexo 01/11/2014	01/11/2014

Figura 38. Inventario de Hardware. Elaboración propia.

Inventario de Software

Mecanismo desarrollado para llevar un control claro y preciso acerca de los elementos de software de la empresa según los criterios o campos clave del área.

Figura 39

N	Aplicación	Descripción	Tipo de licencia	Tipo
1	AutoCAD	Aplicación de dibujo técnico. Usado por el área Planeamiento,	Licenciado	Especializado
2	ArcGis	tratamiento, diseño, publicación e impresión de información geográfica. Usado por el área de Geología y Exploraciones	Licenciado	Especializado
3	FUSION VER.8 (GDMS)	Software de modelamiento Geológico. Usado por el área de	Licenciado	Especializado
4	STUDIO RM	Software de modelamiento Geológico. Usado por el área de	Licenciado	Especializado
5	Microsoft Office 2016	Software base de ofimática. Usado por todas las áreas	Licenciado	Estandar
6	SAP	Software de procesos. Usado por todas las áreas	Licenciado	Estandar
7	CORE PROFILE	Modelamiento Geológico. Usado por el área de Geología	Licenciado	Especializado
8	MULTITEST	Software para test de aptitudes. Usado por el área de	Licenciado	Especializado
9	Goldsim	Balance de agua. Usado por el área de Planta	Licenciado	Especializado
10	ADOBE READER	Visualizador de archivos pdf. Usado por todas las áreas	Libre, shareware	Estandar
11	MINESIGHT	Modelamiento Geológico. Usado por el área de Geología	Licenciado	Especializado
12	PRIMO PDF	Creador de archivos pdf. Usado por todas las áreas	Libre, shareware	Estandar
13	DWG TrueView 2014	Visualizador de archivos dwg. Usado por todas las áreas	Libre, freeware	Estandar
14	Google earth	Permite visualizar múltiple cartografía. Usado por el área de Planeamiento, Geología, Medio Ambiente	Libre, freeware	Especializado
15	McAfee	Antivirus. Usado por todas las áreas	Licenciado	Estandar
16	AXXON NEXT	Software para administración y monitoreo de cámaras. Usado	Licenciado	Especializado
17	Withtittle	Software utilizado para realizar estimaciones de recursos y reservas. Usado por el área de Planeamiento	Licenciado	Especializado
18	WINRAR	Programa compresor y descompresor. Usado por todas las	Licenciado, trialware	Estandar
19	SOFTWARE NEC	Programa para administrar vía wifi proyectores NEC. Usado	Licenciado	Estandar
20	TREMBLE BUSSINES CENTER	Programa para almacenar puntos topográficos. Usado por	Licenciado	Especializado
21	VLC	Reproductor multimedia. Usado por todas las áreas	Libre, freeware	Estandar
22	CLEANER	Microsoft Windows mediante la eliminación de los archivos innecesarios y las entradas inválidas del registro de Windows. Usado por todas las áreas	Libre, freeware	Estandar
23	C_CURE 9000	Software que administra tranquera para el ingreso a	Licenciado	Especializado
24	GEMCOM	Software utilizado para el cálculo de polígonos. Usado por el	Licenciado	Especializado
25	CISCO IP COMMUNICATOR	en un teléfono IP Cisco dotado de todas las funciones con el que realizar y recibir llamadas. Usado el área de Recursos	Licenciado	Especializado
26	SGEMS	Software de modelamiento Geológico. Usado por el área de	Licenciado	Especializado
27	POLYCOM REALPRESENCE DESKTOP	Software utilizado para videoconferencia. Usado por Sistemas y demás áreas de acuerdo a la necesidad	Licenciado	Especializado
28	OMNITREND	recogidos por VIBEXPERT, . Usado por el área de Mantenimiento	Licenciado	Especializado

Figura 39. Inventario de Software. Elaboración propia.

Filtrado MAC

Mecanismo implementado para el control de acceso a las redes inalámbricas de la empresa, con el fin de mantener un control con el uso de las redes.

Figura 41

The screenshot displays the Cisco Security configuration interface for MAC Filtering. The 'Local MAC Filters' section contains a table with the following data:

MAC Address	Profile Name	Interface	IP Address	Description
00:1e:65:de:e8:68	Pucamarca-Standart	management	unknown	DETECTOR TORMENTAS
00:21:0e:01:de:94	Pucamarca-Corporativo	management	unknown	FTC Sistema (Sistema Islander)
00:21:6a:f7:ca:51	Pucamarca-Guest-Contratistas	management	unknown	LSALAS-ANDES
00:21:8b:98:18:4e	Pucamarca-Standart	management	unknown	SEGURIDAD INDUCCIONES
00:21:8b:de:70:60	Any WLAN	management	unknown	TINYPRUEBACAMARAS - TI
00:22:88:02:14:78	Any WLAN	management	unknown	MOTION METRICS - MINSUR - MINA
00:23:14:34:a9:fc	Any WLAN	management	unknown	BACKUP - MINSUR
00:23:14:35:08:94	Any WLAN	management	unknown	TS10 BKC TIC - MINSUR
00:28:68:36:ea:25	Pucamarca-Standart	management	unknown	PUCEXPLO1 LAP - EXPLORACIONES
00:28:68:73:81:79	Pucamarca-Caldero	management	unknown	Kslnha - kps
00:28:68:8f:11:b4	Pucamarca-Guest-Contratistas	management	unknown	MCHIQUE - EXPLORACIONES
00:28:68:8b:5a:6b	Pucamarca-Guest-Contratistas	management	unknown	WSANCHEZ - FERREYROS
00:28:68:eb:a0:1e	Pucamarca-Guest-Contratistas	management	unknown	NRODRIGUEZ-FERREYROS
00:0a:0f:33:19:aa	Pucamarca-Standart	management	unknown	PUCASHERMITA-OC2 - MINSUR TABLE
00:0a:0f:33:34:a8	Pucamarca-Standart	management	unknown	TABLET_GEOLOGIA - MINSUR
04:4e:a7:04:ce:54	Any WLAN	management	unknown	TV SALA CHECOCOLLO
04:4e:a7:04:d6:94	Any WLAN	management	unknown	TV - SALA CALDERO
08:ed:b9:04:6d:75	Pucamarca-Guest-Contratistas	management	unknown	MRAMOS - PEGASUS
0c:2c:54:ca:f1:84	Any WLAN	management	unknown	SOLARWINDS MOBILE
0c:54:15:2a:5f:12	Pucamarca-Standart	management	unknown	JCHAVEZ - MINSUR
0c:54:15:2a:5f:21	Any WLAN	management	unknown	BACKUP 2019 TIC
0c:54:15:2a:5f:49	Any WLAN	management	unknown	BACKUP SIS
0c:54:15:2a:5f:8a	Pucamarca-VIP	management	unknown	RCORSINO - MINSUR
0c:54:15:2a:5f:90	Pucamarca-Standart	management	unknown	CAPONTE - MINSUR
0c:54:15:2a:5f:a8	Pucamarca-Standart	management	unknown	JMUNOZ02 - LAPTOP MINSUR
0c:54:15:2a:5f:b2	Any WLAN	management	unknown	JVAYAMA - MINSUR
0c:54:15:2a:5f:b7	Pucamarca-Standart	management	unknown	EZAPANA - LAPTOP MINSUR
0c:54:15:2a:5f:c6	Pucamarca-Standart	management	unknown	AANDOA - MINSUR
0c:54:15:2a:5f:d0	Pucamarca-Standart	management	unknown	NESTEBAN - MINSUR
0c:54:15:2a:5f:d5	Pucamarca-Standart	management	unknown	FARCE - Minsur
0c:54:15:2a:5f:f3	Pucamarca-Standart	management	unknown	JEFESPLANTA - MINSUR
0c:54:15:35:b3:b7	Pucamarca-Standart	management	unknown	MSJAREZ - LAPTOP MINSUR

Figura 41. Filtrado MAC. Elaboración propia.

4.2 MARCO METODOLÓGICO

Se realizó un estudio experimental que implica determinar dos variables dependientes y una variable independiente, en un pre test y un pos test.

Se usó una metodología de tipo correlacional ya que se cuantificará el grado de relación existente entre las variables en más de un tiempo determinado, se medirá la variable aparentemente relacionada y estudiará la correlación antes y después de aplicar cambios en la variable independiente.

El instrumento fue aplicado a los trabajadores de la unidad minera Pucamarca - Minsur, durante el periodo de mayo del 2018 hasta abril del 2019. Se realizó uso de instrumentos como:

- Observación

Durante la investigación se observó atentamente el proceso de gestionar la seguridad de la información, se recopiló toda la información posible y gracias a esto fue posible tener un panorama más amplio de los problemas estudiados.

- Entrevista

Se elaboró una entrevista estructurada (anexo x) para recabar información en forma verbal, a través de una serie de preguntas elaboradas en base al análisis del problema. Se seleccionaron a los 08 principales líderes de área de la empresa, los cuales son usuarios del

área de TIC y que proporcionaron datos importantes para la investigación. Se realizó la entrevista de manera individual y presencial con los involucrados asegurándose de intercambiar toda la información posible acerca del estado de las TIC en la unidad minera Pucamarca.

- Encuesta

Se elaboró una encuesta estructurada (anexo x) con ítems normalizados y confiables luego de un juicio de expertos, la encuesta podría ser el método de investigación con la capacidad de responder a problemas tanto en términos descriptivos como en términos de relación de variables, luego de la recopilación de información sistemática, según un diseño previamente definido que se cerciore del rigor de la información recopilada como comenta Buendía Eisman, Colás Bravo y Hernández Pina (1998). De esta manera, se puede utilizar para brindar descripciones de los objetos de estudio, detectar comportamientos y relaciones entre las características descritas y definir relaciones entre eventos específicos.

4.2.1 INSTRUMENTOS

El instrumento principal utilizado fue la encuesta estructurada, la cual se elaboró conteniendo ítems de los indicadores de las 3 variables, como comenta Durán Toro y Bernárdez Jiménez (2002).

- Participación de usuario
- Planificación del sistema de información
- Desempeño de los mecanismos de seguridad de la información

La entrevista fue presencial con personal de diferentes sub áreas y se usara para tener un mejor panorama del avance de la investigación. Según Sabino (1992) define a la entrevista, es una manera puntual de interacción social desde un punto de vista metódico, la entrevista tiene por objeto recolectar datos para un estudio.

La encuesta se elaboró en referencia a las 3 variables en estudio y está conformado por preguntas de carácter anónimo con de alternativas múltiples siguiendo como base la escala de Likert. El cuestionario permite explorar la opinión de una población y los puntajes vigentes de una sociedad, tópicos de trascendencia científica y de importancia en las poblaciones democráticas como comenta Grasso (2016).

Tabla 24
Descripción de indicadores

Indicador	Descripción
Participación en el uso de herramientas de seguridad de la información de su empresa	El grado de compromiso de las personas del área en conocer y usar sus herramientas de seguridad de la información
Participación en la seguridad de los SI	El grado de compromiso de las personas del área en definir sus herramientas de seguridad informática
Participación en la identificación del riesgo en TI	El grado de compromiso de las personas del área en identificar sus riesgos de seguridad de la información
Participación en proyectos tecnológicos	El grado de compromiso de las personas del área en definir sus requerimientos en proyectos tecnológicos
Participación en la ejecución de pruebas de control	El grado de compromiso de las personas del área dar su aprobación a los requerimientos de sus sistemas
Control al SI	El grado de compromiso de la empresa en hacer partícipes a las áreas involucradas para definir los requisitos de sus sistemas de información
Control de recursos de infraestructura tecnológica	El grado de compromiso de la empresa en controlar y gestionar sus productos de hardware
Control de recursos de software	El grado de compromiso de la empresa en controlar y gestionar sus productos de software
Metodología de implementación	El grado de compromiso de la empresa en evaluar, implementar y mantener metodologías de desarrollo de sistemas
Estrategia de SI	El grado de compromiso de la empresa en hacer partícipes a las áreas involucradas para la planificación de sus sistemas de información
Control y procedimientos de acceso al SI	El grado de desempeño de los mecanismos de seguridad para gestionar y controlar los archivos documentarios del área
Segregación de funciones en el SI	El grado de desempeño de los mecanismos de seguridad para gestionar y controlar los sistemas de información implementados en la empresa
Políticas de seguridad y acceso al sistema	El grado de desempeño de los mecanismos de seguridad para gestionar y controlar la seguridad de la información de la empresa algún estándar internacional

Nota: Elaboración propia.

La encuesta desarrollada consta de 13 ítems, agrupados en 13 dimensiones para las variables 01 variables, se aplicó individualmente con un tiempo aproximado de 10 minutos.

Tabla 25
Preguntas por indicador

Indicador	Ítem en cuestionario
Participación en el uso de herramientas de seguridad de la información de su empresa	1.Participa en capacitaciones acerca del uso de las herramientas de seguridad informática de su área
Participación en la seguridad de los SI	2.Tienen en cuenta su opinión para el diseño de los sistemas de seguridad informática de su empresa
Participación en la identificación del riesgo en TI	3.Participa identificando riesgos en los sistemas informáticos que usa
Participación en proyectos tecnológicos	4.Tienen en cuenta su opinión para la automatización en proyectos tecnológicos de la empresa
Participación en la ejecución de pruebas de control	5.Participa en pruebas/ certificación de los sistemas informáticos a implementar
Control al SI	6.En la planificación de proyectos, hay supervisión del área de TIC en lo que respecta al ámbito tecnológico
Control de recursos de infraestructura tecnológica	7.Cree que la empresa planifica y ejerce control de los recursos de infraestructura tecnológica
Control de recursos de software	8.Cree que la empresa planifica y ejerce control de los recursos de software
Metodología de implementación	9.Considera que hay una metodología para la implementación de sistemas de información
Estrategia de SI	10.Cree que los SI son producto del análisis de proyectos tecnológicos a fin de apoyar las estrategias de la empresa
Control y procedimientos de acceso al SI	11.Se encuentra satisfecho con los SI de su área, percibe un adecuado control
Segregación de funciones en el SI	12. Según su área considera alta la concentración de funciones de los SI de su área
Políticas de seguridad y acceso al sistema	13. Existen políticas y normas implementadas que mejoran el desempeño del sistema y de los usuarios

Nota: Elaboración propia.

Los indicadores definidos, así como la encuesta estructurada elaborada, es confiable, dado que se validó a través de una encuesta de juicio de expertos, los profesionales seleccionados son de amplia experiencia de los sectores Minería y Tecnologías de la información.

Los ítems son cuantificados según la escala de Likert y dado que no han sido redactados en el mismo sentido han sido codificados de modo que una puntuación mayor vaya asociada a una actitud positiva y viceversa.

Los códigos correspondientes a los 13 ítems son los siguientes:

- TD: Total desacuerdo
- D: Desacuerdo
- N: Neutro
- A: Acuerdo
- TA: Totalmente de acuerdo

Para estudiar la correlación entre la “Planificación De Los Sistemas de Información” en el “Desempeño de Mecanismos de Seguridad de la Información”, se realizó una pre prueba al inicio del estudio y una post prueba luego de implementar cambios en la variable independiente.

Se utilizó una entrevista con 5 preguntas para medir la “Planificación De Los Sistemas de Información” luego de determinar sus respectivos indicadores .Las preguntas del cuestionario se encuentran a cada indicador definido, las cuales de las veremos a continuación:

Tabla 26
Variables, indicadores e ítems

Variable	Indicador	Ítem en cuestionario
Participación del usuario	Participación en el uso de herramientas de seguridad de la información de su empresa	Participa en capacitaciones acerca del uso de las herramientas de seguridad informática de su área
	Participación en la seguridad de los SI	Tienen en cuenta su opinión para el diseño de los sistemas de seguridad informática de su empresa
	Participación en la identificación del riesgo en TI	Participa identificando riesgos en los sistemas informáticos que usa
	Participación en proyectos tecnológicos	Tienen en cuenta su opinión para la automatización en proyectos tecnológicos de la empresa
	Participación en la ejecución de pruebas de control	Participa en pruebas/ certificación de los sistemas informáticos a implementar
Planificación de los SI	Control al SI	En la planificación de proyectos, hay supervisión los puntos correspondientes a TIC
	Control de recursos de infraestructura tecnológica	Cree que la empresa planifica y ejerce control de los recursos de infraestructura tecnológica
	Control de recursos de software	Cree que la empresa planifica y ejerce control de los recursos de software
	Metodología de implementación	Considera que hay una metodología para la implementación de sistemas de información
	Estrategia de SI	Cree que los SI son producto del análisis de proyectos tecnológicos a fin de apoyar las estrategias de la empresa
Desempeño de mecanismos de seguridad de la información	Control y procedimientos de acceso al SI	Se encuentra satisfecho con los SI de su área, percibe un adecuado control
	Segregación de funciones en el SI	Según su área considera alta la concentración de funciones de los SI de su área
	Políticas de seguridad y acceso al sistema	Existen políticas y normas implementadas que mejoran el desempeño del sistema y de los usuarios

Nota: Elaboración propia.

La recolección de datos se llevó a cabo en base a las preguntas de la tabla número 24, se realizó el cuestionario y se pidió a los expertos seleccionados su opinión, sobre el diseño del cuestionario para el cuestionario. Anexo 03.

4.3 TIPO DE DISEÑO

La metodología utilizada en esta investigación será de tipo correlacional dado que se cuantificará el nivel de relación que existe entre estas variables en un pre prueba y post prueba, es decir dos tiempos determinados, se medirá cada variable posiblemente relacionada y estudiará la correlación. El diseño de la investigación será experimental, transversal – correlacional como indica

Buendía Eisman, Colás Bravo y Hernández Pina (1998)

4.4 POBLACIÓN

La población según Balestrini Acuña (2006) comenta es la población total de los seres o elementos a los cuales se refiere la investigación, dicho de otra manera, todos los elementos que vamos a investigar, es por ello también se le conoce como universo

Tabla 27

Estratos de población

ESTRATOS POR AREAS DE NEGOCIO EN MINSUR PUCAMARCA -TACNA	
PERSONAL STAFF MINSUR	89
PERSONAL STAFF CONTRATISTA	19
PERSONAL TECNICO MINSUR	16
PERSONAL TECNICO CONTRATISTA	8
TOTAL MUESTRA	139

Nota: Elaboración propia

La población seleccionada para el estudio son los colaboradores de la unidad minera Pucamarca Minsur, dicha población está conformada por el personal profesional, técnico que mantiene contacto con factores de TIC de la empresa dado que estas personas se verán afectadas por la investigación.

4.5 MUESTRA

La muestra es un segmento representativo de una población, cuyas características o peculiaridades deben repetirse en ella, lo más parecido posible como indica Balestrini Acuña (2006).

La muestra será seleccionada a partir de la población de los colaboradores de la unidad minera Pucamarca Minsur en la ciudad de Tacna, asumiendo un 95% de grado confianza. En este caso consideraremos una máxima variabilidad (p y q serán 0.5) dado que no hay antecedentes específicos de esta investigación,

Fórmula:

Población finita: $n = \frac{Z^2 * p * q * N}{e^2 * (N-1) + Z^2 * p * q}$

Dónde:

$n = ?$	(Tamaño de la muestra)
$N = 139$	(Población o universo)
$Z = 1.96$	(Nivel de confianza)
$p = 0.5$	(Probabilidad a favor)
$q = 0.5$	(Probabilidad en contra)
$e = 0.5$	(Error muestral)

$$n = \frac{(1.96)^2 * (0.5) * (0.5) * 139}{(0.5)^2 * (139-1) + (1.96)^2 * (0.5) * (0.5)}$$
$$n = 102$$

Tabla 28
Estratos de muestra

ESTRATOS POR AREAS DE NEGOCIO EN MINSUR PUCAMARCA	
PERSONAL STAFF MINSUR	78
PERSONAL STAFF CONTRATISTA	12
PERSONAL TECNICO MINSUR	11
PERSONAL TECNICO CONTRATISTA	1
TOTAL MUESTRA	102

Nota: Elaboración propia

4.6 RECOLECCION DE INFORMACIÓN

El cuestionario se efectuó en las distintas instalaciones de la unidad minera

Pucamarca:

- Oficinas ADR
- Oficinas Planta
- Oficinas Mantenimiento
- Oficinas Truckhop
- Almacén – logística

Un cuestionario por cada trabajador de área según nuestra muestra, haciendo un total de 102 encuestados, los cuales son usuarios finales de los sistemas de información y por lo tanto tienen información valiosa para medir la participación del usuario, la planificación de los sistemas de información y el desempeño de los mecanismos de seguridad de la información.

Los cuestionarios fueron llenados según las preguntas elaboradas con la finalidad de evaluar el desempeño de los mecanismos de seguridad de la información en la empresa, lo cual se puede ver en el anexo 05.

Para la evaluación se aplicaron 02 pruebas en distintos tiempos en las distintas instalaciones de la Unidad Minera Pucamarca, obteniendo un desempeño favorable luego mejorar la gestión de seguridad de la información (anexo 05).

4.7 RESULTADOS PARA LA VARIABLE D1

La variable dependiente “Participación Del Usuario” indica que tanto los usuarios toman parte de conocer sus procesos a automatizar en la implementación de un sistema de información.

Dados los últimos eventos en la empresa, los usuarios deben ser capacitados en los riesgos de informática a los que están expuestos, así como participar en el diseño de controles o herramientas para minimizar estos riesgos. Toda automatización a implementarse deberá ser validada por ellos dado que son los usaran estas herramientas.

4.7.1. Validación y confiabilidad del instrumento

A través del juicio de expertos se validaron los ítems del cuestionario, este grupo está constituido por profesionales con amplia experiencia en Minería y Tecnologías de la información, la cual se puede ver en el anexo 14.

Para el cálculo de la confiabilidad, se usó el procedimiento de consistencia interna, usando como formula el coeficiente de alfa de Cronbach.

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum_{i=1}^k \sigma_i^2}{\sigma_t^2}\right)$$

Donde:

α : Coeficiente del alfa de Cronbach

k: Número de preguntas

σ_{i2} : Varianza del puntaje por cada pregunta

σ_{t2} : Varianza del puntaje total por cada trabajador de la muestra piloto.

Como se aprecia a continuación las respuestas se encuentran en una escala del 1-5 considerando.

- 1 : Nada adecuado
- 2: Poco adecuado
- 3: Adecuado
- 4: Bastante adecuado
- 5: Muy adecuado

En la tabla 29 se muestran los resultados de la validación de los ítems por juicio de expertos y en la tabla 31 el coeficiente del alfa de Cronbach obtenido con ayuda de MS Excel. Según Ruiz Bolívar (2013) la confiabilidad está asociada a la idea de que los resultados obtenidos con el instrumento en caso determinado, bajo ciertas condiciones, serían exactamente iguales si volviéramos a medir el mismo rasgo bajo las mismas condiciones.

El cuestionario fue validado por el juicio de 13 expertos y se usó análisis estadístico de Coeficiente de Cronbach.

Tabla 29
Resultados de la validación de los ítems

EXPERTO	P1	P2	P3	P4	P5
1	4	5	4	5	4
2	4	5	4	5	5
3	3	3	3	4	4
4	4	5	4	5	4
5	4	5	4	5	5
6	3	3	3	4	4
7	4	5	4	5	4
8	4	5	4	5	5
9	3	3	3	4	4
10	4	5	4	5	4
11	4	5	4	5	3
12	3	3	3	4	4
13	4	5	4	5	3

Nota: Elaboración propia

Tabla 30
Estadístico de confiabilidad

SUMA DE VARIANZA DE LOS ÍTEMS	2.02564103
VARIANZA TOTAL DE ÍTEMS	6.43589744
K	5

Nota: Elaboración propia

$$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S_T^2} \right]$$

$\alpha =$ 5/(5-1) * [1 - (2.026/6.436)]
 $\alpha =$ 1.25 * [1- 0.395]
 $\alpha =$ 0.857

Tabla 31
Alfa de Cronbach

ALFA DE CRONBACH	=0,857
Nº DE ELEMENTOS	5

Nota: Elaboración propia

Figura 42



Figura 42. Intervalo de confiabilidad de Cronbach. *Elaboración propia.*

Como se puede apreciar, el resultado tiene un valor α de 0,857 y es muy cercano a 1, lo que significa que el actual instrumento tiene un grado alto de confiabilidad, dándole la confianza necesaria para la recolección de datos.

4.7.2. Diseño de presentación de datos

A continuación, se presenta los resultados del cuestionario en lo que respecta a la variable "Participación Del Usuario" aplicado a cada integrante de la muestra, el cual se encuentra dividido en 5 partes ya que cada pregunta está asignada a un indicador.

a) Con respecto a la dimensión “Participación en el uso de herramientas de seguridad de la información de su empresa”

En la tabla 32 se aprecia los resultados de la “Participación Del Usuario” aplicado en la Unidad Minera Pucamarca, según la dimensión “Participación en el uso de herramientas de seguridad de la información de su empresa” con una calificación promedio de 4.225.

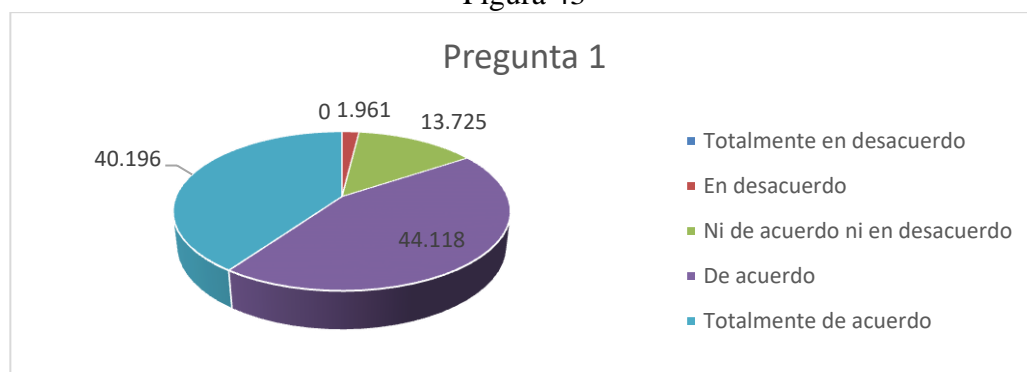
Tabla 32

Participación en el uso de herramientas de seguridad de la información

PREGUNTA 1	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	2	1,961	4
Ni de acuerdo ni en desacuerdo	14	13,725	42
De acuerdo	45	44,118	180
Totalmente de acuerdo	41	40,196	205
TOTAL	102	100%	431
PROMEDIO		4,225	

Nota: Elaboración propia

Figura 43



En la figura 43 se puede visualizar la distribución de los porcentajes según la dimensión de “Participación en el uso de herramientas de seguridad de la información de su empresa”, se observa que existe un porcentaje de 40.196% que se encuentra totalmente de acuerdo y el 44.118% está de acuerdo; con el cumplimiento de la dimensión.

b) Con respecto a la dimensión “Participación en la seguridad de los sistemas de información”

En la tabla 33 se aprecia los resultados de la “Participación Del Usuario” aplicado en la Unidad Minera Pucamarca, según la dimensión “Participación en la seguridad de los sistemas de información” con una calificación promedio de 4.137.

Tabla 33

Participación En La Seguridad De Los Sistemas De Información

PREGUNTA 2	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	2	1,961	4
Ni de acuerdo ni en desacuerdo	17	16,667	51
De acuerdo	48	47,059	192
Totalmente de acuerdo	35	34,314	175
TOTAL	102	100%	422
PROMEDIO		4,137	

Nota: Elaboración propia

Figura 44

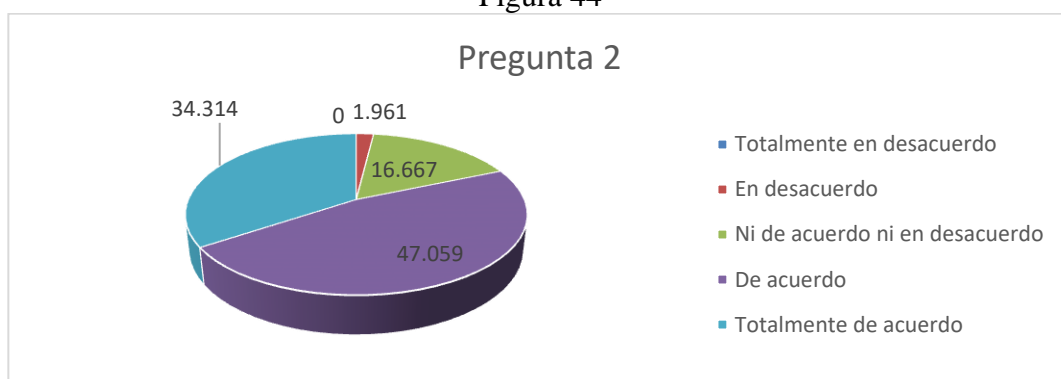


Figura 44. Participación En La Seguridad De Los Sistemas De Información. Elaboración propia.

En la figura 44 se puede visualizar la distribución de los porcentajes en referencia a la dimensión de “Participación En La Seguridad De Los Sistemas De Información”, se observa que existe un porcentaje de 34.314% que se encuentra totalmente de acuerdo y el 47.059% está de acuerdo; con el cumplimiento de la dimensión.

c) Con respecto a la dimensión “Participación en la identificación del riesgo en TI”

En la tabla 34 se aprecia los resultados de la “Participación Del Usuario” aplicado en la Unidad Minera Pucamarca, según la dimensión “Participación en la identificación del riesgo en TI” con una calificación promedio de 4.059.

Tabla 34

Participación en la identificación del riesgo en TI

PREGUNTA 3	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	1	0,98	2
Ni de acuerdo ni en desacuerdo	24	23,529	72
De acuerdo	45	44,118	180
Totalmente de acuerdo	32	31,373	160
TOTAL	102	100%	414
PROMEDIO		4,059	

Nota: Elaboración propia

Figura 45

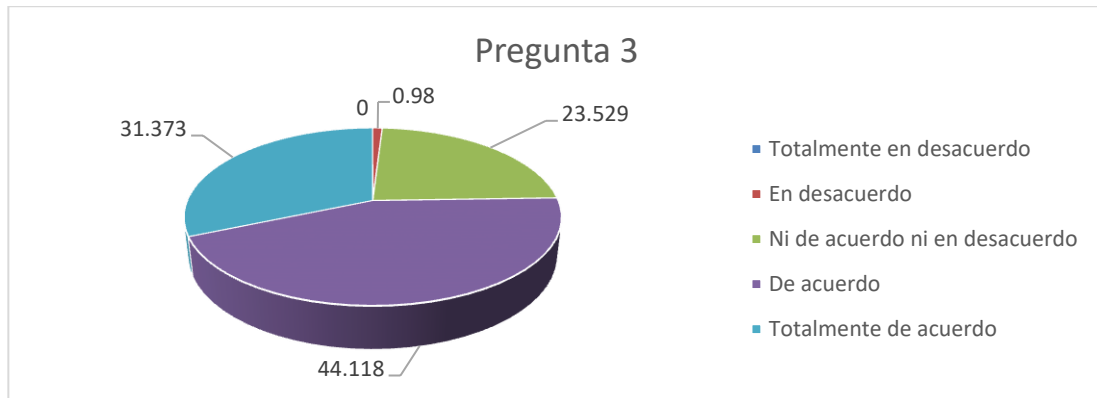


Figura 45. Participación en la identificación del riesgo en TI. Elaboración propia.

En la figura 45 se puede visualizar la distribución de los porcentajes en referencia a la dimensión de “Participación en la identificación del riesgo en TI”, se observa que existe un porcentaje de 31.373% que se encuentra totalmente de acuerdo y el 44.118% está de acuerdo; con el cumplimiento de la dimensión.

d) Con respecto a la dimensión “Participación en proyectos tecnológicos”

En la tabla 35 se aprecia los resultados de la “Participación Del Usuario” aplicado en la Unidad Minera Pucamarca, según la dimensión “Participación en proyectos tecnológicos” con una calificación promedio de 4.049.

Tabla 35

Participación en proyectos tecnológicos

PREGUNTA 4	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	3	2,941	6
Ni de acuerdo ni en desacuerdo	20	19,608	60
De acuerdo	48	47,059	192
Totalmente de acuerdo	31	30,392	155
TOTAL	102	100%	413
PROMEDIO		4,049	

Nota: Elaboración propia

Figura 46

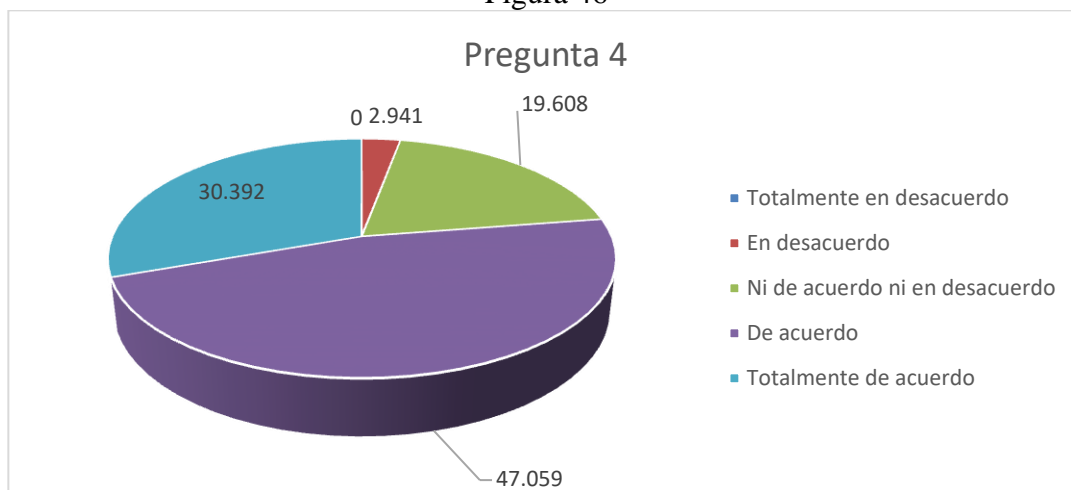


Figura 46. Participación en proyectos tecnológicos. Elaboración propia.

En la figura 46 se puede visualizar la distribución de los porcentajes según la dimensión de “Participación en proyectos tecnológicos”, se observa que existe un porcentaje de 30.392% que se encuentra totalmente de acuerdo y el 47.059% está de acuerdo; con el cumplimiento de la dimensión.

e) Con respecto a la dimensión “Participación en la ejecución de pruebas de control”

En la tabla 36 se aprecia los resultados de la “Participación Del Usuario” aplicado en la Unidad Minera Pucamarca, según la dimensión “Participación en la ejecución de pruebas de control” con una calificación promedio de 4.098.

Tabla 36

Participación en la ejecución de pruebas de control

PREGUNTA 5	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	0	0	0
Ni de acuerdo ni en desacuerdo	22	21,569	66
De acuerdo	48	47,059	192
Totalmente de acuerdo	32	31,373	160
TOTAL	102	100%	418
PROMEDIO		4,098	

Nota: Elaboración propia

Figura 47

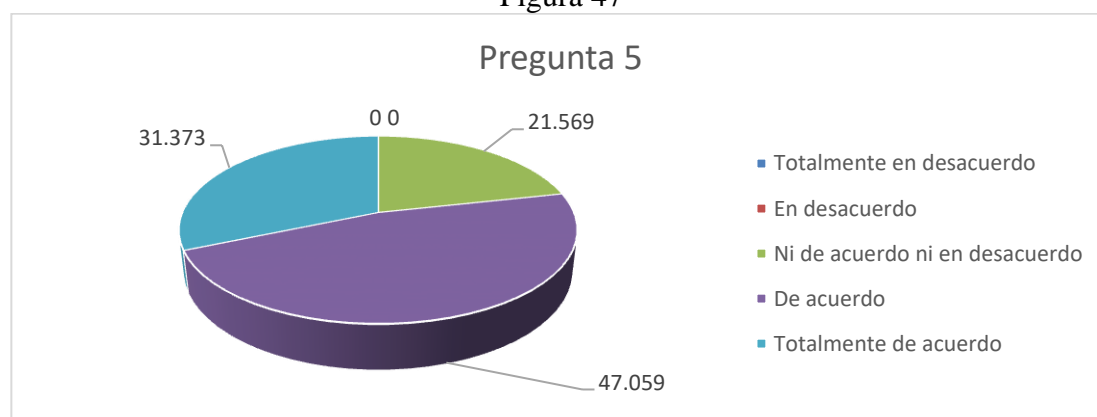


Figura 47. Participación en ejecución de pruebas de control. Elaboración propia.

En la figura 47 se puede visualizar la distribución de los porcentajes en referencia a la dimensión de “Participación en ejecución de pruebas de control”, se observa que existe un porcentaje de 31.373% que se encuentra totalmente de acuerdo y el 47.059% está de acuerdo; con el cumplimiento de

la dimensión.

4.8 RESULTADOS PARA LA VARIABLE D2

La variable dependiente “Planificación de los Sistemas de información” indica que tanto la empresa toma parte de conocer sus sistemas de información a implementar, así como que tanto vela por su integridad, disponibilidad y confidencialidad.

Dados los últimos eventos en la empresa, la empresa ser consciente de la importancia de la seguridad de la información, debe tener una correcta gestión de software y hardware, así como ser partícipe de los sistemas de información que se encuentran implementándose alineándose a buenas prácticas o metodologías con alto grado de aceptación.

4.8.1. Validación y confiabilidad del instrumento

A través del juicio de expertos se validaron los ítems del cuestionario, este grupo está constituido por profesionales con amplia experiencia en Minería y Tecnologías de la información, la cual se puede ver en el anexo 14.

Para el cálculo de la confiabilidad, se usó el procedimiento de consistencia interna, usando como formula el coeficiente de alfa de Cronbach.

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum_{i=1}^k \sigma_i^2}{\sigma_t^2}\right)$$

Donde:

α : Coeficiente del alfa de Cronbach

k: Número de preguntas

σ_{i2} : Varianza del puntaje por cada pregunta

σ_{t2} : Varianza del puntaje total por cada trabajador de la muestra piloto.

Como se aprecia a continuación las respuestas se encuentran en una escala del 1-5 considerando.

- 1 : Nada adecuado
- 2: Poco adecuado
- 3: Adecuado
- 4: Bastante adecuado
- 5: Muy adecuado

En la tabla 35 se muestran los resultados de la validación de los ítems por juicio de expertos y en la tabla 37 el coeficiente del alfa de Cronbach obtenido con ayuda de MS Excel.

Según Ruiz Bolívar (2013) la confiabilidad está asociada a la idea de que los resultados provenientes del instrumento en un caso determinado o bajo ciertas circunstancias, serian exactamente iguales si volviéramos a estudiar la misma variable bajo las mismas condiciones.

El cuestionario fue validado por el juicio de 13 expertos y se usó análisis estadístico de Coeficiente de Cronbach.

Tabla 37
Resultados de la validación de los ítems para la variable 2

EXPERTO	P6	P7	P8	P9	P10
1	5	5	5	5	4
2	4	5	4	5	5
3	3	3	3	4	4
4	4	5	4	5	4
5	4	5	4	5	5
6	3	3	3	4	4
7	4	5	4	5	4
8	4	5	4	5	5
9	3	3	3	4	4
10	4	5	4	5	4
11	4	3	4	4	5
12	4	4	4	5	4
13	4	5	4	5	3

Nota: Elaboración propia

Tabla 38
Estadístico de confiabilidad

SUMA DE VARIANZA	2.1025641
VARIANZA TOTAL ITEMS	6.07692308
K	5

Nota: Elaboración propia

$$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S_T^2} \right]$$

$$\alpha = 5/(5-1) * [1 - (2.103/ 6.077)]$$

$$\alpha = 1.25 * [1- 0.346]$$

$$\alpha = 0.818$$

a) Con respecto a la dimensión “Control al sistema de información”

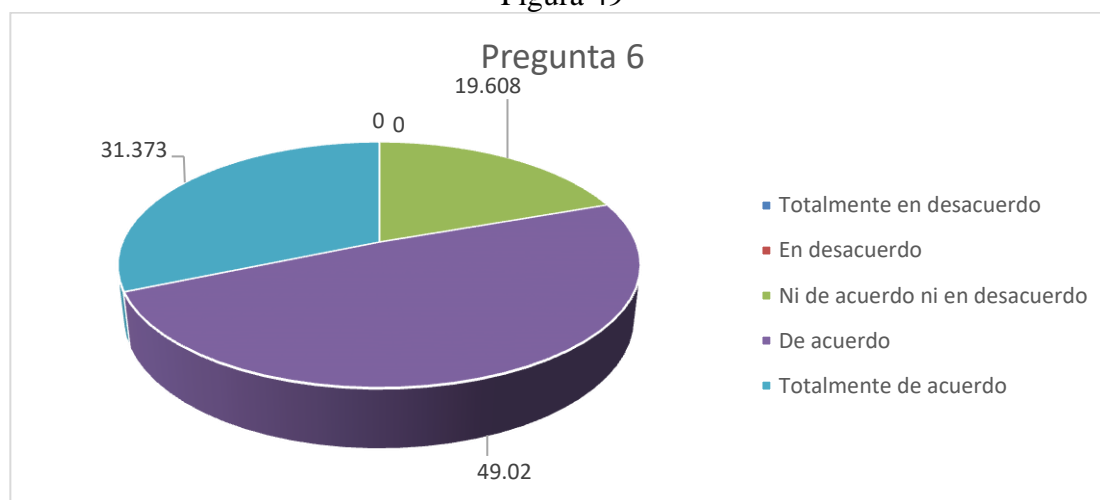
En la tabla 40 se aprecia los resultados de la “Planificación de los sistemas de información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Control al sistema de información” con una calificación promedio de 4.118.

Tabla 40
Control al sistema de información

PREGUNTA 6	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	0	0	0
Ni de acuerdo ni en desacuerdo	20	19,608	60
De acuerdo	50	49,02	200
Totalmente de acuerdo	32	31,373	160
TOTAL	102	100%	420
PROMEDIO		4,118	

Nota: Elaboración propia

Figura 49



En la figura 49 se puede visualizar la distribución de los porcentajes según la dimensión de “Control al sistema de información”, se observa que existe un porcentaje de 31.373% que se encuentra totalmente de acuerdo y el 49.02% está de acuerdo; con el cumplimiento de la dimensión.

b) Con respecto a la dimensión “Control de recursos de infraestructura tecnológica”

En la tabla 41 se aprecia los resultados de la “Planificación de los sistemas de información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Control de recursos de infraestructura tecnológica” con una calificación promedio de 4.294.

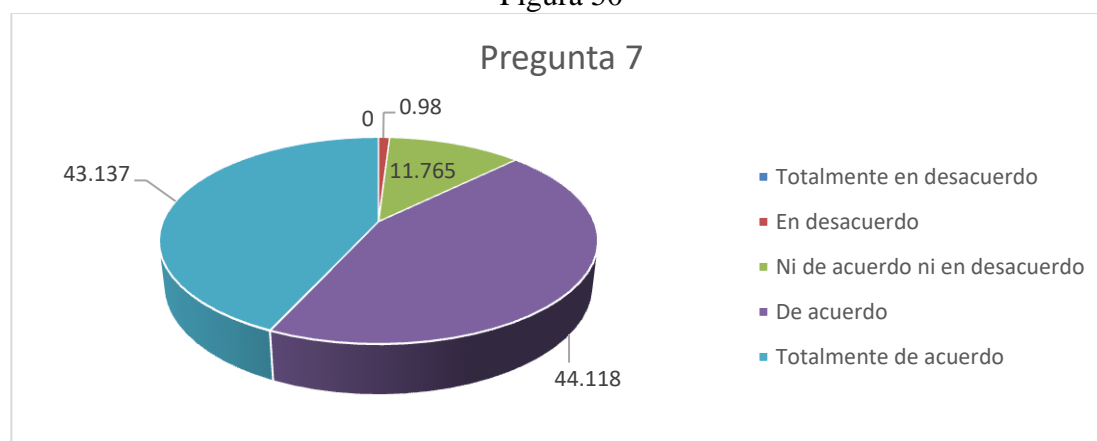
Tabla 41

Control de recursos de infraestructura tecnológica

PREGUNTA 7	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	1	0,98	2
Ni de acuerdo ni en desacuerdo	12	11,765	36
De acuerdo	45	44,118	180
Totalmente de acuerdo	44	43,137	220
TOTAL	102	100%	438
PROMEDIO		4,294	

Nota: Elaboración propia

Figura 50



En la figura 50 se puede visualizar la distribución de los porcentajes según la dimensión de “Control de recursos de infraestructura tecnológica”, se observa que existe un porcentaje de 43.137% que se encuentra totalmente de acuerdo y el 44.118% está de acuerdo; con el cumplimiento de la dimensión.

c) Con respecto a la dimensión “Control de recursos de software”

En la tabla 42 se aprecia los resultados de la “Planificación de los sistemas de información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Control de recursos de software” con una calificación promedio de 4.255.

Tabla 42
Control de recursos de software

PREGUNTA 8	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	5	4,902	10
Ni de acuerdo ni en desacuerdo	9	8,824	27
De acuerdo	43	42,157	172
Totalmente de acuerdo	45	44,118	225
TOTAL	102	100%	434
PROMEDIO		4,255	

Nota: Elaboración propia

Figura 51

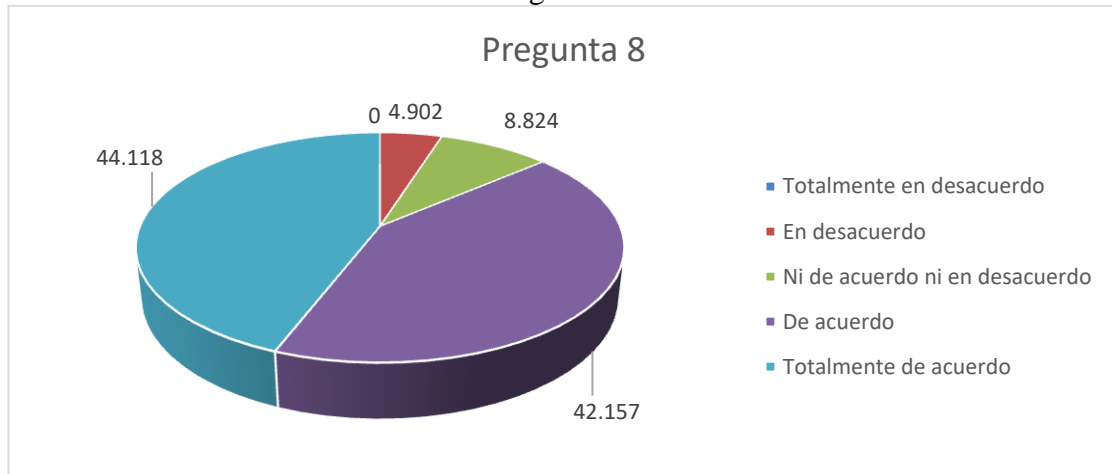


Figura 51. Control de recursos de software. Elaboración propia.

En la figura 51 se puede visualizar la distribución de los porcentajes según la dimensión de “Control de recursos de software”, se observa que existe un porcentaje de 44.118% que se encuentra totalmente de acuerdo y el 42.157% está de acuerdo; con el cumplimiento de la dimensión.

d) Con respecto a la dimensión “Metodología de implementación”

En la tabla 43 se aprecia los resultados de la “Planificación de los sistemas de información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Metodología de implementación” con una calificación promedio de 4.284.

Tabla 43

Metodología de implementación

PREGUNTA 9	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	1	0,98	2
Ni de acuerdo ni en desacuerdo	11	10,784	33
De acuerdo	48	47,059	192
Totalmente de acuerdo	42	41,176	210
TOTAL	102	100%	437
PROMEDIO		4,284	

Nota: Elaboración propia

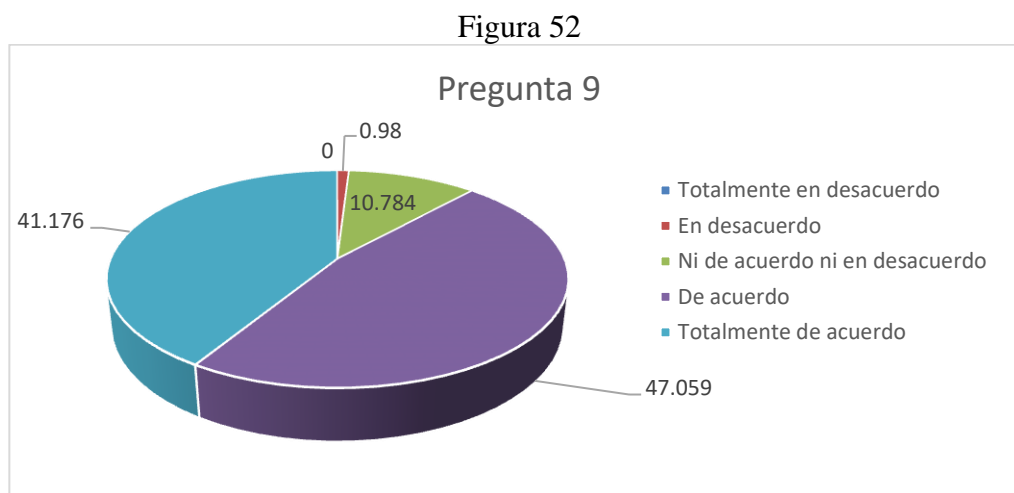


Figura 52. Metodología de implementación. Elaboración propia.

En la figura 52 se puede visualizar la distribución de los porcentajes según la dimensión de “Metodología de implementación”, se observa que existe un porcentaje de 41.176% que se encuentra totalmente de acuerdo y el 47.059% está de acuerdo; con el cumplimiento de la dimensión.

e) Con respecto a la dimensión “Estrategia del sistema de información”

En la tabla 44 se aprecia los resultados de la “Planificación de los sistemas de información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Estrategia del sistema de información” con una calificación promedio de 4.333.

Tabla 44

Estrategia del sistema de información

PREGUNTA 10	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	2	1,961	4
Ni de acuerdo ni en desacuerdo	12	11,765	36
De acuerdo	38	37,255	152
Totalmente de acuerdo	50	49,02	250
TOTAL	102	100%	442
PROMEDIO		4,333	

Nota: Elaboración propia

Figura 53

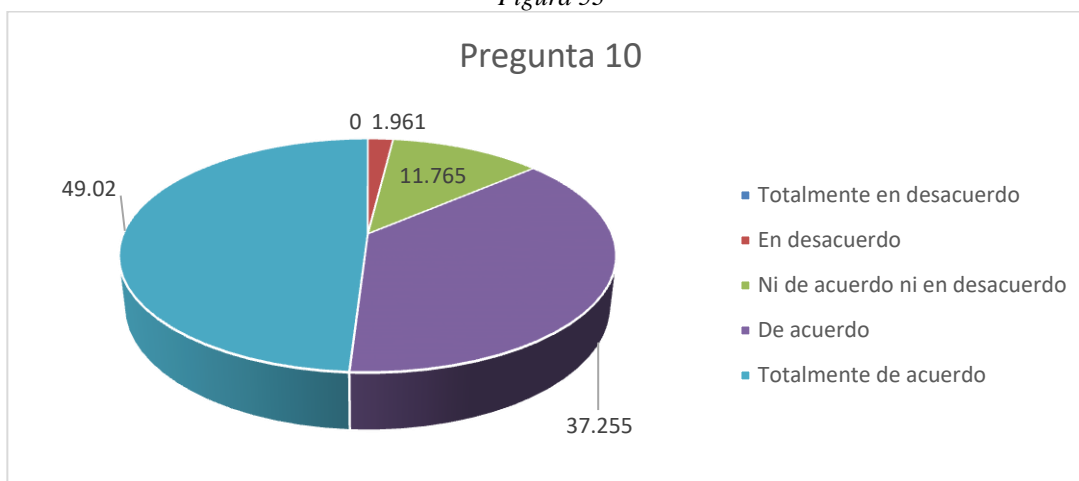


Figura 53. Estrategia del sistema de información. Elaboración propia.

En la figura 53 se puede visualizar la distribución de los porcentajes según la dimensión de “Estrategia del sistema de información”, se observa que existe un porcentaje de 49.02% que se encuentra totalmente de acuerdo y el

37.255% está de acuerdo; con el cumplimiento de la dimensión.

4.9 RESULTADOS PARA LA VARIABLE INDEPENDIENTE

La variable dependiente “Desempeño de Mecanismos de Seguridad de la Información” indica el grado de madurez de herramientas o controles de seguridad de la información aplicados en la gestión de seguridad de la información de la empresa

Dados los últimos eventos en la empresa, es necesario evaluar si la gestión de seguridad de la información se está llevando de manera correcta, y al aplicar cambios en las variables dependiente, analizar si existe algún cierto grado de mejora en la gestión de seguridad de la información.

4.9.1. Validación y confiabilidad del instrumento

A través del juicio de expertos se validaron los ítems del cuestionario, este grupo está constituido por profesionales con amplia experiencia en Minería y Tecnologías de la información, la cual se puede ver en el anexo 14.

Para el cálculo de la confiabilidad, se usó el procedimiento de consistencia interna, usando como formula el coeficiente de alfa de Cronbach.

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum_{i=1}^k \sigma_i^2}{\sigma_t^2}\right)$$

Donde:

α : Coeficiente del alfa de Cronbach

k: Número de preguntas

σ_{i2} : Varianza del puntaje por cada pregunta

σ_{t2} : Varianza del puntaje total por cada trabajador de la muestra piloto.

Como se aprecia a continuación las respuestas se encuentran en una escala del 1-5 considerando.

- 1: Nada adecuado
- 2: Poco adecuado
- 3: Adecuado
- 4: Bastante adecuado
- 5: Muy adecuado

En la tabla 43 se muestran los resultados de la validación de los ítems por juicio de expertos y en la tabla 45 el coeficiente del alfa de Cronbach obtenido con ayuda de MS Excel.

Según Ruiz Bolívar (2013), la confiabilidad está asociada a la idea de que los resultados obtenidos con el instrumento en caso determinado, bajo ciertas condiciones, serían exactamente iguales si volviéramos a medir el mismo rasgo bajo las mismas condiciones. El cuestionario fue validado por el juicio de 13 expertos y se usó análisis estadístico de Coeficiente de Cronbach.

Tabla 45

Resultados de la validación de los ítems para la variable

EXPERTO	P11	P12	P13
1	5	5	5
2	4	5	4
3	3	3	3
4	4	5	4
5	4	5	4
6	3	3	3
7	4	5	4
8	4	5	4
9	3	3	3
10	4	5	4
11	4	5	3
12	4	3	4
13	4	5	4

Nota: Elaboración propia

Tabla 46

Estadístico de confiabilidad

SUMA DE VARIANZA	1.58974359
VARIANZA TOTAL ITEMS	3.66666667
K	3

Nota: Elaboración propia

$$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S_T^2} \right]$$

$$\alpha = \frac{3}{3-1} * [1 - (1.59 / 3.667)]$$

$$\alpha = 1.5 * [1 - 0.433]$$

$$\alpha = 0.85$$

Tabla 47
Alfa de Cronbach

ALFA DE CRONBACH	=0,85
Nº DE ELEMENTOS	14

Nota: Elaboración propia

Figura 54

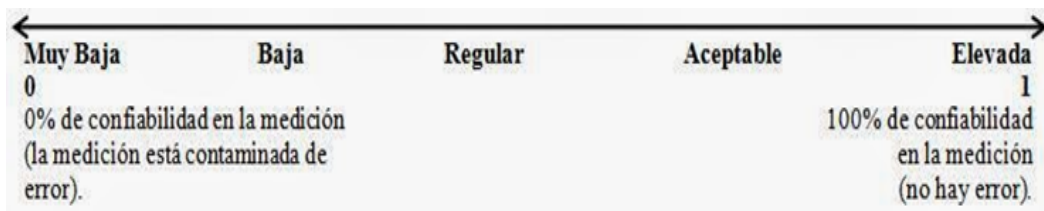


Figura 54. Intervalo de confiabilidad de Cronbach. Elaboración propia.

Como se puede apreciar, el resultado tiene un valor α de 0,85 y es muy cercano a 1, lo que significa que el actual instrumento tiene un grado alto de confiabilidad, dándole la confianza necesaria para la recolección de datos.

4.9.2. Diseño de presentación de datos

A continuación, se presenta los resultados del cuestionario en lo que respecta a la variable “Planificación de los sistemas de información” aplicado a cada integrante de la muestra, el cual se encuentra dividido en 5 partes ya que cada pregunta está asignada a un indicador.

a) Con respecto a la dimensión “Control y procedimientos de acceso al sistema de información”

En la tabla 48 se aprecia los resultados del “Desempeño de los mecanismos de seguridad de la información” aplicado en la UM Pucamarca, según la dimensión “Control al sistema de información” con una calificación promedio de 4.265.

Tabla 48

Control al sistema de información

PREGUNTA 11	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	3	2,941	6
Ni de acuerdo ni en desacuerdo	12	11,765	36
De acuerdo	42	41,176	168
Totalmente de acuerdo	45	44,118	225
TOTAL	102	100%	435
PROMEDIO		4,265	

Nota: Elaboración propia

Figura 55

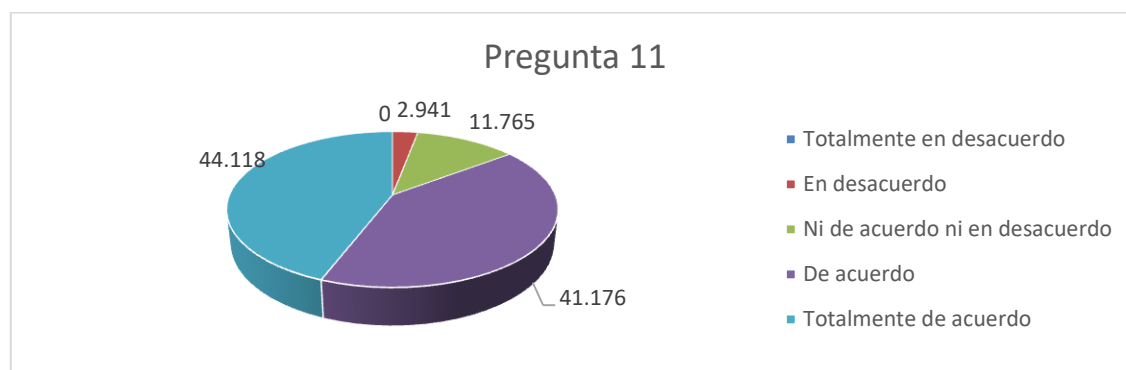


Figura 55. Control al sistema de información. Elaboración propia.

En la figura 55 se puede visualizar la distribución de los porcentajes en referencia a la dimensión de “Control al sistema de información”, se observa que existe un porcentaje de 44.118% que se encuentra totalmente de acuerdo

y el 41.176% está de acuerdo; con el cumplimiento de la dimensión.

b) Con respecto a la dimensión “Segregación de funciones en el sistema de información”

En la tabla 49 se aprecia los resultados del “Desempeño de los mecanismos de seguridad de la información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Segregación de funciones en el sistema de información” con una calificación promedio de 4.363.

Tabla 49

Segregación de funciones en el sistema de información

PREGUNTA 12	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	1	0,98	2
Ni de acuerdo ni en desacuerdo	15	14,706	45
De acuerdo	32	31,373	128
Totalmente de acuerdo	54	52,941	270
TOTAL	102	100%	445
PROMEDIO		4,363	

Nota: Elaboración propia

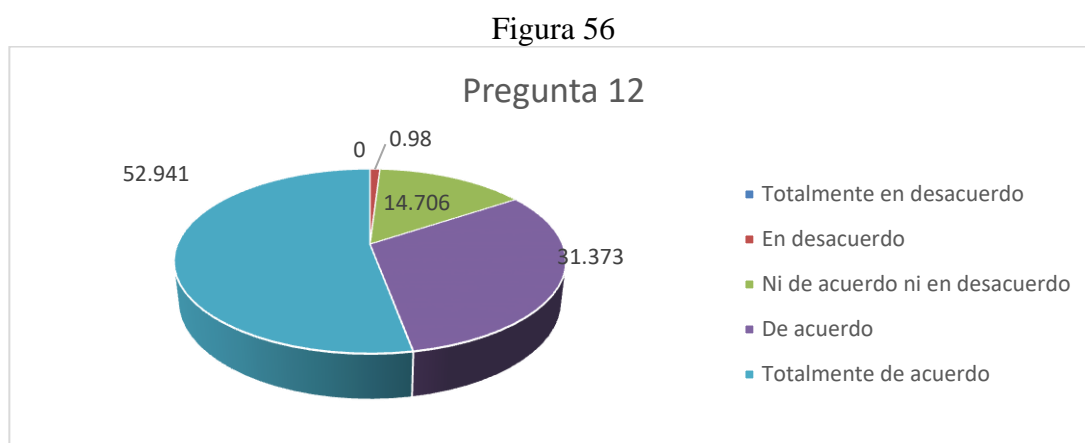


Figura 56. Segregación de funciones en el sistema de información. Elaboración propia.

En la figura 56 se puede visualizar la distribución de los porcentajes según la dimensión de “Segregación de funciones en el sistema de información”, se observa que existe un porcentaje de 52.941% que se encuentra totalmente de

acuerdo y el 31.373% está de acuerdo; con el cumplimiento de la dimensión.

c) Con respecto a la dimensión “Políticas de seguridad y acceso al sistema”

En la tabla 50 se aprecia los resultados de la “Desempeño de los mecanismos de seguridad de la información” aplicado en la Unidad Minera Pucamarca, según la dimensión “Políticas de seguridad y acceso al sistema” con un promedio de 4.304 de puntaje.

Tabla 50

Políticas de seguridad y acceso al sistema

PREGUNTA 13	FRECUENCIA	PORCENTAJE	PUNTAJE
Totalmente en desacuerdo	0	0	0
En desacuerdo	0	0	0
Ni de acuerdo ni en desacuerdo	18	17,647	54
De acuerdo	35	34,314	140
Totalmente de acuerdo	49	48,039	245
TOTAL	102	100%	439
PROMEDIO		4,304	

Nota: Elaboración propia

Figura 57

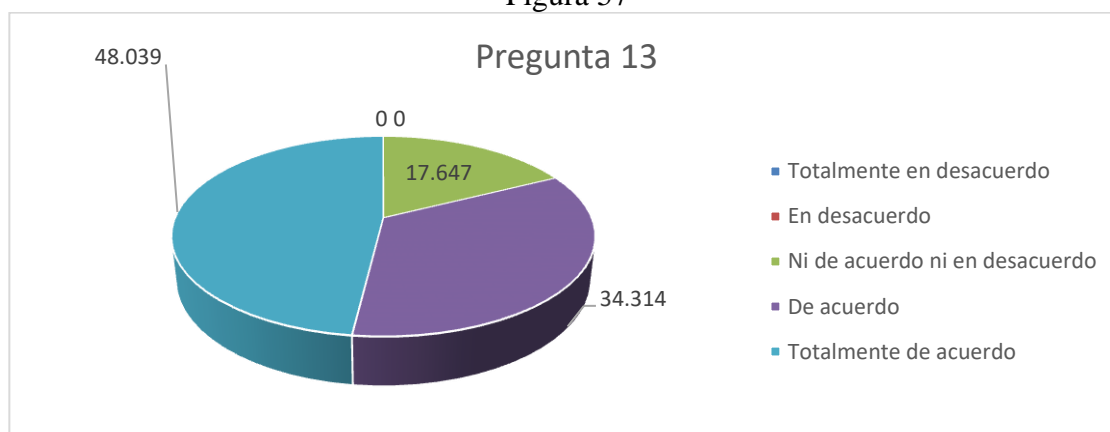


Figura 57. Políticas de seguridad y acceso al sistema. Elaboración propia.

En la figura 57 se puede visualizar la distribución de los porcentajes según la dimensión de “Políticas de seguridad y acceso al sistema”, se observa que existe un porcentaje de 48.039% que se encuentra totalmente de acuerdo y el

34.314% está de acuerdo; con el cumplimiento de la dimensión.

4.6 CONTRASTE DE HIPÓTESIS

Luego de desarrollar el planteamiento metodológico y factores teóricos del estudio, procederemos a entrelazar la información recopilada, procesarla, interpretarla, con el fin de contrastar las hipótesis definidas en la presente investigación.

Con la finalidad de facilitar el entendimiento de los resultados obtenidos, la información se presentará a través de un análisis de correlación existente entre los indicadores y variables, resultado una interpretación por ítem.

Totalizando los datos procesados por variable se hará posible la aceptación o rechazo de las hipótesis de la investigación.

Primera sub hipótesis

H_0 : La participación del usuario no influye en el desempeño de los mecanismos de seguridad de la información en la empresa.

H_1 : La participación del usuario influye en el desempeño de los mecanismos de seguridad de la información en la empresa.

Paso 1: Establecemos la hipótesis:

$$H_0: p > 0.05$$

$$H_1: p < 0.05$$

Paso 2: Establecemos el nivel de significancia:

$$\alpha = 0,05$$

Paso 3: La investigación busca relacionar dos variables cuantitativas ordinales con muestras dependientes, por lo cual calculamos la correlación del puntaje de ambas variables (anexo x) según el coeficiente de correlación de Spearman donde:

$$r_s = 1 - \frac{6\sum D^2}{N(N^2 - 1)}$$

Donde:

- r_s : coeficiente de correlación por rangos de Spearman
- D: diferencia entre las parejas de datos
- N: número de parejas de datos

Paso 4: Obtenemos los datos de correlación:

Tabla 51
Correlación de Spearman

		Correlaciones	
		PUPRE	PUPOS
Rho de Spearman PUPRE	Coeficiente de correlación	1,000	,361**
	Sig. (unilateral)	.	,000
	N	102	102
PUPOS	Coeficiente de correlación	,361**	1,000
	Sig. (unilateral)	,000	.
	N	102	102

** La correlación es significativa en el nivel 0,01 (unilateral).

Nota: Elaboración propia

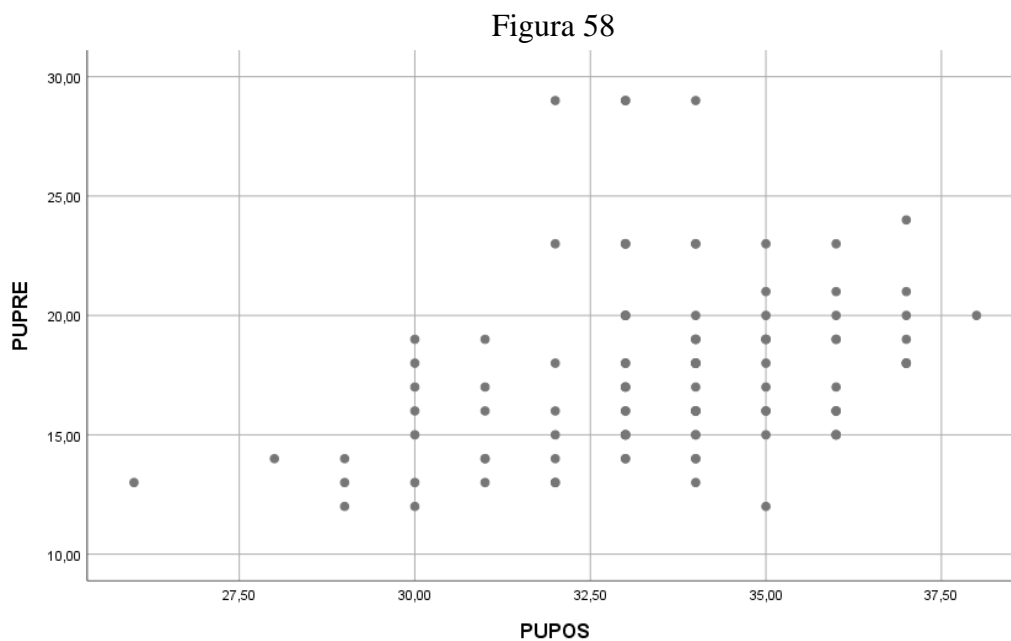


Figura 58. Diagrama de dispersión de correlación. Elaboración propia.

Paso 5: Interpretar los datos obtenidos

El valor de Rho de Spearman tiene un valor de 0.361 y r_s tiene un valor 0.000095 siendo menor al nivel de significancia 0.05, por lo cual rechazamos H_0 y aceptamos H_1 con un 95% de confianza.

Por lo tanto, se concluye que la participación del usuario influye en el desempeño de los mecanismos de seguridad de la información en la empresa.

Segunda sub hipótesis

H_0 : No existe una relación entre la planificación de los sistemas de información y el desempeño de los mecanismos de seguridad de información en la empresa.

H_1 : Existe una relación entre la planificación de los sistemas de información y el desempeño de los mecanismos de seguridad de información en la empresa.

Paso 1: Establecemos la hipótesis:

$$H_0: p > 0.05$$

$$H_1: p < 0.05$$

Paso 2: Establecemos el nivel de significancia:

$$\alpha = 0,05$$

Paso 3: La investigación busca relacionar dos variables cuantitativas ordinales con muestras dependientes, por lo cual calculamos la correlación del puntaje de ambas variables (anexo x) según el coeficiente de correlación de Spearman donde:

$$r_s = 1 - \frac{6\sum D^2}{N(N^2 - 1)}$$

Donde:

- r_s : coeficiente de correlación por rangos de Spearman
- D: diferencia entre las parejas de datos
- N: número de parejas de datos

Paso 4: Obtenemos los datos de correlación:

Tabla 52
Correlación de Spearman

		Correlaciones	
		PSPRE	PSPOS
Rho de Spearman PSPRE	Coeficiente de correlación	1,000	,351**
	Sig. (unilateral)	.	,000
	N	102	102
PSPOS	Coeficiente de correlación	,351**	1,000
	Sig. (unilateral)	,000	.
	N	102	102

** . La correlación es significativa en el nivel 0,01 (unilateral).

Nota: Elaboración propia

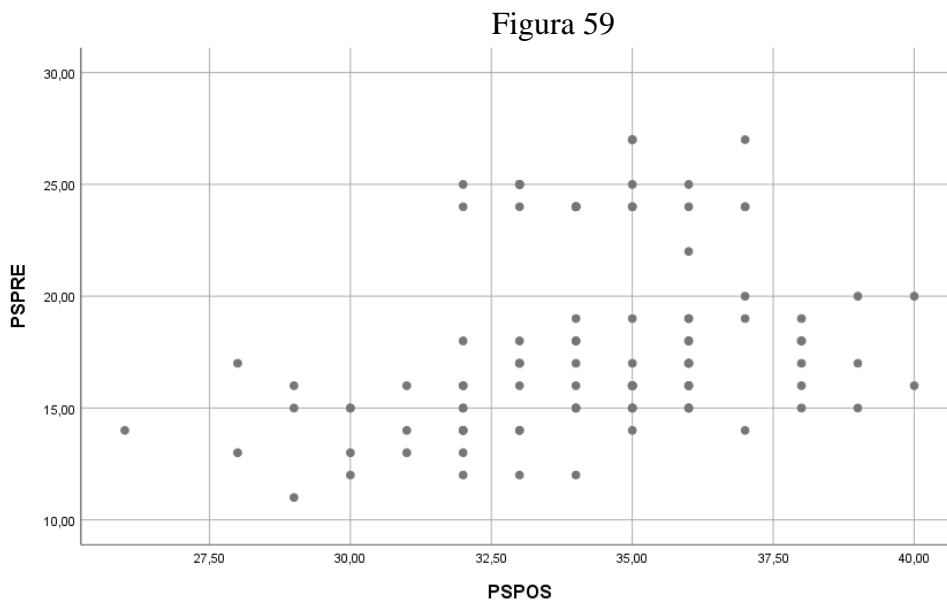


Figura 59. Diagrama de dispersión de correlación. Elaboración propia.

Paso 5: Interpretar los datos obtenidos

El valor de Rho de Spearman tiene un valor de 0.351 y r_s tiene un valor 0.000146 siendo menor al nivel de significancia 0.05, por lo cual rechazamos H_0 y aceptamos H_1 con un 95% de confianza.

Por lo tanto, se concluye que la participación del usuario influye en el desempeño de los mecanismos de seguridad de la información en la empresa.

Hipótesis Global

H₀: No existe un mejor desempeño de los mecanismos de seguridad de la información en la empresa luego de analizar y mejorar la relación con sus variables más importantes

H₁: Existe un mejor desempeño de los mecanismos de seguridad de la información en la empresa luego de analizar y mejorar la relación con sus variables más importantes

Con los resultados de las sub hipótesis, se compararon las medias de los indicadores resultantes, en dos periodos distintos de tiempo.

Paso 1: Establecemos la hipótesis:

$$H_0: x_{pre} \geq x_{post}$$

$$H_1: x_{pre} \leq x_{post}$$

Paso 2: Calcularemos las medias de puntaje de la muestra de variable en los dos periodos de tiempo:

$$x_{pre} = 6,598$$

$$x_{pos} = 12,931$$

Paso 3: Comparamos el valor de las medias:

$$6.598 \leq 12.931$$

Paso 4: Interpretar los datos obtenidos

La media del puntaje pos prueba es mayor al puntaje pre prueba por lo cual rechazamos H_0 y aceptamos H_1 y se puede decir, que la variable “Desempeño de los mecanismos de seguridad de la información” ha mejorado su desempeño en un 95.98%.

CONCLUSIONES

PRIMERA

El desempeño de los mecanismos de seguridad de la información tenía un bajo desempeño; se mejoraron los mecanismos actuales, así como se implementaron algunos nuevos y se evidencia una mejora significativa desde que se implementaron estas herramientas de control y gestión de seguridad de la información en un 95%.

SEGUNDA

Se observó y comprobó la relación entre la planificación de los sistemas de información y el desempeño de los mecanismos de seguridad de la información a través de un estudio de correlación, mostrando una influencia fuerte y la misma dirección para ambas variables.

TERCERA

Se observó y comprobó la influencia entre la participación del usuario y desempeño de los mecanismos de seguridad de la información a través de un estudio de correlación, mostrando una relación fuerte y la misma dirección para ambas variables.

SUGERENCIAS

PRIMERA

Se recomienda intensificar y ampliar la rutina y contenido del plan de capacitaciones, así como planificar simulacros de eventos que atenten contra la seguridad de la información de la empresa a fin de evaluar el comportamiento del personal.

SEGUNDA

Se recomienda desarrollar un plan estratégico de tecnologías de la información e incluir los representantes de gerencia y las áreas correspondientes a que participen en él.

TERCERA

Se recomienda alinear todos los conceptos, herramientas, controles existentes en la empresa a un modelo de gestión de seguridad de la información que comprenda una mejora continua de su gestión hasta poder establecerse como un Sistema de Gestión de Seguridad de la información acorde a la ISO 27001.

BIBLIOGRAFIA

- Aguilera Lopez, P. (2004). *Seguridad informática*. Madrid.
- Areitio Bertolín, J. (2008). *Seguridad de la información*. Madrid.
- Balestrini Acuña, M. (2006). *Como se elabora el proyecto de investigación*.
Caracas.
- Buendía Eisman, L., Colás Bravo, P., & Hernández Pina, F. (1998). *MÉTODOS DE INVESTIGACIÓN EN PSICOPEDAGOGÍA*. Madrid.
- Chiesa, F. (2004). *Metodología para la selección de sistemas ERP*. Buenos Aires.
- Díaz , J., Harari, I., & Amadeo, A. (2013). *Guía de recomendaciones para diseño de software centrado en el usuario*. Buenos Aires.
- Durán Toro, A., & Bernárdez Jiménez, B. (2002). *Metodología para la Elicitación de requisitos de Sistemas Software*. Sevilla.
- Fernández Alarcon, V. (2006). *Desarrollo de sistemas*. Barcelona.
- García Cervigón Hurtado, A., & Alegre Ramos, M. (2011). *Seguridad Informática*. Madrid.
- Giner de la Fuente, F. (2004). *Los Sistemas de Información en la sociedad del conocimiento*. Madrid.
- Granollers, T., Lorés vidal, J., & Cañas Delgado, J. (2005). *Diseño de sistemas interactivos centrados en el usuario*. Barcelona.
- Grasso, L. (2016). *Encuestas. Elementos para su diseño y análisis*. Buenos Aires: Brujas.
- Hurtado León, I., & Toro Garrido, J. (2005). *Paradigmas y Métodos de*

- investigación*. Valencia.
- INSTITUTE, IT GOVERNANCE. (2007). *COBIT 4.1*. Illinois.
- ISO. (1989). *7498-2*. Switzerland.
- Laudon, K., & Laudon, J. (2004). *Sistemas de información gerencial*. México.
- Martínez Méndez, F. (2004). *Recuperación de información: Modelos, sistemas y evaluación*. Murcia.
- McLeod Raymond, J. (2000). *Sistemas de información gerencial*. México.
- Minsur. (2018). *Memoria Anual 2018*.
- Ramon Rodríguez, J., García Mínguez, J., & Lamarca Orozco, I. (2007). *Gestión de proyectos informáticos: métodos, herramientas y casos*. Barcelona.
- Rey Martin, C. (2000). *LA SATISFACCIÓN DEL USUARIO: UN CONCEPTO EN ALZA*. Barcelona.
- Roa Buendía, J. (2013). *Seguridad informática*. Madrid.
- Ruiz Bolívar, C. (2013). *Instrumentos y Técnicas de Investigación Educativa*. Texas.
- Sabino, C. (1992). *El proceso de investigación*. Buenos Aires.
- Serpbell Bley, A., & Alarcón Cárdenas, L. (2015). *Planificación y control de proyectos*. Santiago.
- Solano Rodríguez, O., García Perez de Lema, D., & Jesus Bernal, J. (2016). *El sistema de información y los mecanismos de seguridad informática en la pyme*. Cartagena.
- Stallings, W. (2001). *Comunicaciones y Redes de Computadores*. Madrid.
- Stallings, W. (2004). *Fundamentos de seguridad en redes*. Madrid.

VAN HAREN PUBLISHING. (2008). *Diseño de servicio basada en ITIL V3*.

Amersfoort.

Vanegas Devia, G. A., & Pardo, C. (2014). Hacia un modelo para la gestión de

TI en Pymes. *Towards a IT risks management model for MSME*, 36.

World Economic Forum. (2015). Mining & Metals in a Sustainable World 2050.

Industry Agenda.

ANEXOS

ANEXO 1 ENTREVISTAS

ENTREVISTA : ESTADO ACTUAL DE LAS TIC EN PUCAMARCA	
Lugar: Unidad Minera Pucamarca Minsur Fecha: 11/09/15	
1. ¿Usted cree que la información relacionada con los sistemas de información de su área, es correcta y nunca ha sido modificada?	Si, solo en el área de gestión. Tiene acceso y son 2 personas.
2. ¿Usted cree que la información relacionada con los sistemas de información de su área, es confidencial y solo puede acceder a ella personal autorizado?	Si, más que algunos otros usuarios acceden, pero solo si TIC de los permisos.
3. ¿Usted cree que la información relacionada con los sistemas de información de su área, es altamente disponible?	Si, puede que fuera de la unidad sea un poco difícil de acceder por la VPN (limitada).
4. ¿Usted cree que los usuarios de las distintas áreas se encuentran al tanto de sus sistemas, aplicaciones y equipos de automatización y su correcto uso?	No totalmente, algunos (nuevos) no están al tanto de los sistemas de su área, así como equipos, en minería hay mucha resistencia al cambio.
5. ¿Usted cree que existe una buena proyección acerca de los recursos de TIC en la empresa?	Estamos en una era de innovación, y va de la mano con TIC, hay una buena proyección pero es necesario aterrizar esos ideas.
6. ¿Se encuentra al tanto de los procedimientos, políticas y tareas que abarca el área de TIC de la empresa?	Si, pero hay algunos no documentados.
7. ¿Usted cree que hay adecuado control de la información en la empresa?	Si, el área de TIC vela por eso.

Ch. A. Gabur

ENTREVISTA : ESTADO ACTUAL DE LAS TIC EN PUCAMARCA	
	Lugar: Unidad Minera Pucamarca Minsur Fecha:
1. ¿Usted cree que la información relacionada con los sistemas de información de su área, es correcta y nunca ha sido modificada?	El asunto de perdidas ultimamente, pero a lo largo de los años se reportaron bastante
2. ¿Usted cree que la información relacionada con los sistemas de información de su área, es confidencial y solo puede acceder a ella personal autorizado?	Libro oculto en modo lectura, todos pueden solo ver solo me da, TIC y generación lo cual se debe cuidar bien.
3. ¿Usted cree que la información relacionada con los sistemas de información de su área, es altamente disponible?	No, no siempre, se han efectuado cortes del servicio por distintas razones (proceder, naturaleza, negligencias)
4. ¿Usted cree que los usuarios de las distintas áreas se encuentran al tanto de sus sistemas, aplicaciones y equipos de automatización y su correcto uso?	No totalmente, existen varios sistemas por los que se paga y no se usan
5. ¿Usted cree que existe una buena proyección acerca de los recursos de TIC en la empresa?	Si hay una buena inversión y proyección pero se deben dirigir correctamente a las necesidades de la empresa
6. ¿Se encuentra al tanto de los procedimientos, políticas y tareas que abarca el área de TIC de la empresa?	No,
7. ¿Usted cree que hay adecuado control de la información en la empresa?	No, se han reportado casos de pérdida de la información



Victor Rivas

 Analista

ANEXO 4 REGISTRO DE CAPACITACIONES

		FORMATO REGISTRO DE ASISTENCIA DE ACTIVIDADES FORMATIVAS		Código: UM-PU-PG-019-F-003 Versión: 0 Fecha de aprobación: 28/08/2014 Páginas: 1
Tema / Actividad <u>Capacitación Teórica y SUSEO</u>				
Area o Equipo <u>Sistemas</u>				
Hora de inicio <u>08:00 pm</u> Hora de Término: <u>08:40 pm</u>				
Fecha <u>10/02/19</u>				
Lugar <u>Sala WIREP / Tiquena</u>				
Facilitador/Responsable <u>Wán Alvarado Espino</u> Firma:				
Nº	Código Personal/DNI	Apellidos y Nombres	Área / Empresa	Firma
1	00793994	Eberth Atencio Ch.	RR-HH / Pegasus	
2	20507225	Rafael Rivas	Pegasus	
3	41819131	ESPINOZA GARCIA FANNH	RR-HH / Pegasus	
4	40695506	Flomoni Drenzo, Edula	RR-HH / Pegasus	
5	40409263	Cauma Wianaca Lucas	RR-HH / Pegasus	
6	40162699	Ordoñez Celque David	RR-HH / Pegasus	
7	00514763	Villabazo Jose	RR-HH / Pegasus	
8	46284470	Gilmer Espinoza P.	RR-HH / Pegasus	
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				

ANEXO 6
RELACION DE PROFESIONALES QUE SE HAN CONSIDERADO COMO
EXPERTOS PARA LA VALIDACION DEL CUESTIONARIO


RELACION DE PROFESIONALES QUE SE HAN CONSIDERADO COMO EXPERTOS PARA LA VALIDACIÓN DEL CUESTIONARIO


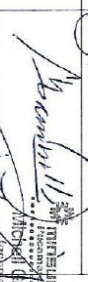

N°	NOMBRES Y APELLIDOS	CARGO	JEFATURA	FIRMA
1	ELIZABETH CORDOVA CORNEJO	JEFE DE LOGISTICA	LOGISTICA	 Jefe Logística.
2	IVAN VELASQUEZ CASTILLO	JEFE DE COSTOS Y PRESUPUESTOS	COSTOS	
3	JORGE SOTELO ESPINOZA	JEFE DE MANTENIMIENTO MECANICO	MANTENIMIENTO	
4	VICTOR RIVADENEIRA RAMAL	ANALISTA DE RIESGOS	RIESGOS	 Victor Rivadeneira Ramal Analista de Riesgos
5	LUIS ZAMUDIO RAMOS	ADMINISTRADOR TI	TIC	 ADMINISTRADOR TI
6	RONALD OJEDA NINA	ESPECIALISTA EN SOPORTE HD	TIC	
7	EDWIN VARGAS GONZALES	ESPECIALISTA EN SOPORTE HD	TIC	
8	JOHN FLORES VILCA	ING. PLANNER DE MANTTO	MANTENIMIENTO	
9	MICHELL GAMBETTA MONTALVO	ING. DE PROYECTOS	PROYECTOS	
10	JOSEPH ROSALES VALDEIGLESIAS	ING. DE PROYECTOS	PROYECTOS	


RELACION DE PROFESIONALES QUE SE HAN CONSIDERADO COMO EXPERTOS PARA LA VALIDACIÓN DEL CUESTIONARIO

N°	NOMBRES Y APELLIDOS	CARGO	INSTITUCIÓN/ÁREA	FIRMA
1	FERNANDO CONTRERAS VELÁSQUEZ	JEFE DE LA UNIDAD DE PROYECTOS	AREA / PLANIFICACION	

RELACION DE PROFESIONALES QUE SE HAN CONSIDERADO COMO EXPERTOS PARA LA VALIDACIÓN DEL CUESTIONARIO

N°	NOMBRES Y APELLIDOS	CARGO	INSTITUCIÓN/ÁREA	FIRMA
1	GINO PARRAVIDINO JACOBO	Ing Sistemas / Consultor TIC	Independiente	

8	JOHN FLORES VILCA	ING. PLANNER DE MANTTO	MANTENIMIENTO	
9	MICHELL GAMBETTA MONTALVO	ING. DE PROYECTOS	PROYECTOS	 <small>INSTITUCIÓN: INSTITUTO NACIONAL DE INVESTIGACIONES Y PROMOCIONES TECNOLÓGICAS NOMBRE: MICHELL GAMBETTA MONTALVO</small>
10	JOSEPH ROSALES VALDEGLESIAS	ING. DE PROYECTOS	PROYECTOS	 <small>INSTITUCIÓN: INSTITUTO NACIONAL DE INVESTIGACIONES Y PROMOCIONES TECNOLÓGICAS NOMBRE: JOSEPH ROSALES VALDEGLESIAS</small>

10	ERICK REATEGUI	JEFE DE MEDIO AMBIENTE	MEDIO AMBIENTE	
----	----------------	------------------------	----------------	---

RELACION DE PROFESIONALES QUE SE HAN CONSIDERADO COMO EXPERTOS PARA LA VALIDACIÓN DEL CUESTIONARIO

Nº	NOMBRES Y APELLIDOS	CARGO	JEFATURA	FIRMA
1	LUIS ESTEBAN INGAROCA	GERENTE DE OPERACIONES	GERENCIA	
2	JIMMY BENDEZU RIOS	ADMINISTRADOR TI	TIC	 <small> INSTITUCION PROYECTO JIMMY BENDEZU RIOS Administrador TI </small>
3	MIGUEL GUARDAMINO GUTIERREZ	JEFE DE COSTOS Y PRESUPUESTOS	COSTOS	
4	LUIS ZAMUDIO RAMOS	COORDINADOR DE SERVICIOS HD	TIC	
5	RONALD OJEDA NINA	ESPECIALISTA EN SOPORTE HD	TIC	
6	JUAN MARISCAL VILLAVICENCIO	JEFE DE LOGISTICA	LOGISTICA	
7	LUIS ARANA SUAREZ	SUPERINTENDENTE DE MANTTO	MANTENIMIENTO	
8	JOHN FLORES VILCA	ING. PLANNER DE MANTTO	MANTENIMIENTO	

ANEXO 7 ANALISIS DE CONFIABILIDAD DEL INSTRUMENTO

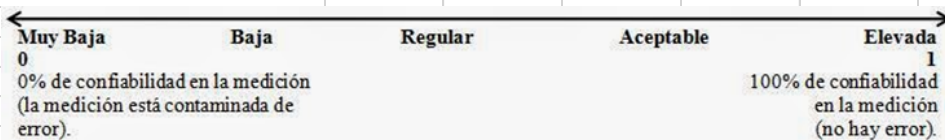
VARIABLE: PARTICIPACIÓN DEL USUARIO

N	EXPERTO	P1	P2	P3	P4	P5	TOTAL
1	LUIS ESTEBAN INGAROCA	4	5	4	5	4	22
2	ERICK REATEGUI	4	5	4	5	5	23
3	JORGE SOTELO	3	4	3	4	4	18
4	LUIS ZAMUDIO RAMOS	4	5	4	5	4	22
5	JESUS VARGAS	4	5	4	5	5	23
6	ELIZABETH CORDOVA	3	4	5	3	4	19
7	LUIS ARANA SUAREZ	4	5	5	5	4	23
8	JOHN FLORES VILCA	5	5	4	5	4	23
9	MICHELL GAMBETTA MONTALVO	4	3	3	4	4	18
10	JOSEPH ROSALES VALDEIGLESIAS	4	5	4	5	4	22
11	FERNANDO CONTRERAS VELÁSQUEZ	4	5	4	5	3	21
12	GINO PARRAVIDINO	3	3	3	3	4	16
13	VICTOR RIVADENEIRA	4	4	4	4	4	20
TOTAL		50	58	51	58	53	
PROMEDIO		3,84615385	4,46153846	3,92307692	4,46153846	4,07692308	
DESVIACION ESTANDAR		0,5547002	0,77625003	0,64051262	0,77625003	0,49354812	
VARIANZA		0,30769231	0,6025641	0,41025641	0,6025641	0,24358974	

SUMA DE VARIANZA	2,16666667
VARIANZA TOTAL ITEMS	5,52564103
K	5

$$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S_r^2} \right]$$

$\alpha=$	5/(5-1) * [1 - (2.167/5.526)]
$\alpha=$	1.25 * [1- 0.392]
$\alpha=$	0,76



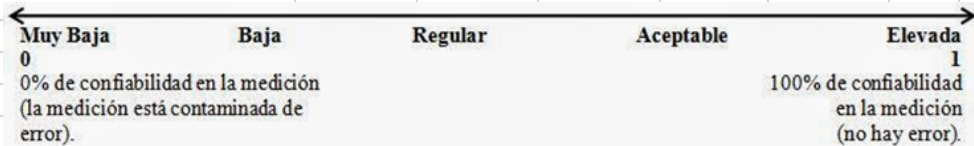
VARIABLE: PLANIFICACIÓN DE SISTEMAS

N	EXPERTO	P6	P7	P8	P9	P10	TOTAL
1	LUIS ESTEBAN INGAROCA	5	5	5	5	5	25
2	ERICK REATEGUI	4	5	5	5	5	24
3	JORGE SOTELO	5	5	4	5	5	24
4	LUIS ZAMUDIO RAMOS	5	5	4	5	5	24
5	JESUS VARGAS	5	5	5	5	5	25
6	ELIZABETH CORDOVA	3	4	5	4	4	20
7	LUIS ARANA SUAREZ	5	4	5	4	5	23
8	JOHN FLORES VILCA	5	4	5	5	5	24
9	MICHELL GAMBETTA MONTALVO	5	5	5	5	5	25
10	JOSEPH ROSALES VALDEIGLESIAS	5	5	5	5	4	24
11	FERNANDO CONTRERAS VELÁSQUEZ	4	3	4	4	5	20
12	GINO PARRAVIDINO	4	4	4	5	4	21
13	VICTOR RIVADENEIRA	3	4	3	4	5	19
TOTAL		58	58	59	61	62	
PROMEDIO		4,46153846	4,46153846	4,53846154	4,6923077	4,76923077	
DESVIACION ESTANDAR		0,77625003	0,66022529	0,66022529	0,4803845	0,43852901	
VARIANZA		0,6025641	0,43589744	0,43589744	0,2307692	0,19230769	

SUMA DE VARIANZA	1,8974359
VARIANZA TOTAL ITEMS	4,57692308
K	5

$$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S_T^2} \right]$$

$\alpha =$	$5/(5-1) * [1 - (1,898/4,577)]$
$\alpha =$	$1.25 * [1 - 0.346]$
$\alpha =$	0,732



VARIABLE: DESEMPEÑO DE MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

N	EXPERTO	P11	P12	P13	TOTAL
1	LUIS ESTEBAN INGAROCA	5	4	5	14
2	ERICK REATEGUI	4	5	4	13
3	JORGE SOTELO	4	3	4	11
4	LUIS ZAMUDIO RAMOS	4	5	4	13
5	JESUS VARGAS	4	5	5	14
6	ELIZABETH CORDOVA	5	3	5	13
7	LUIS ARANA SUAREZ	4	4	4	12
8	JOHN FLORES VILCA	5	4	5	14
9	MICHELL GAMBETTA MONTALVO	4	3	5	12
10	JOSEPH ROSALES VALDEIGLESIAS	5	5	5	15
11	FERNANDO CONTRERAS VELÁSQUEZ	4	5	3	12
12	GINO PARRAVIDINO	4	3	4	11
13	VICTOR RIVADENEIRA	5	5	4	14
TOTAL		57	54	57	
PROMEDIO		4,38461538	4,15384615	4,38461538	
DESVIACION ESTANDAR		0,50636968	0,89871703	0,65044364	
VARIANZA		0,25641026	0,80769231	0,42307692	

SUMA DE VARIANZA	1,48717949
VARIANZA TOTAL ITEMS	1,57692308
K	3

$$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S_T^2} \right]$$

$\alpha =$	$3/(3-1) * [1 - (1.59/3.667)]$
$\alpha =$	$1.5 * [1 - 0.433]$
$\alpha =$	0,85

←					→	
Muy Baja	Baja	Regular	Aceptable	Elevada		
0				1		
0% de confiabilidad en la medición (la medición está contaminada de error).				100% de confiabilidad en la medición (no hay error).		

ANEXO 8 CUESTIONARIO DE VALIDACIÓN PARA LOS ÍTEMS

1. ESCRIBA SUS DATOS EN LAS CASILLAS CORRESPONDIENTE

Apellidos y Nombres :

Empresa/ Institución :

Cargo :

A continuación, se solicita su opinión respecto a si usted está de acuerdo con los ítems, para la validación del cuestionario de la investigación denominada "Estudio del desempeño de mecanismos de seguridad de la información en empresas mineras nacionales, Perú 2019".
Se está clasificando los ítems acorde a su indicador y su variable

Para ello solo deberá marcar con una cruz (x) en la columna que considere la correcta según su opinión, en cada uno de los ítems.

Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

OPINIÓN SOBRE LOS ITEMS ELABORADOS SEGÚN INDICADORES

Variable	Indicador	Ítem en cuestionario	Respuestas de los ítems	Su opinión				
				1	2	3	4	5
Participación del usuario (VD)	Participación en el uso de herramientas de seguridad de la información de su empresa	Participa en capacitaciones acerca del uso de los sistemas informáticos de su área						
	Participación en la seguridad de los sistemas de información	Tienen en cuenta su opinión para el diseño de los sistemas de seguridad informática de su empresa						
	Participación en la identificación del riesgo en TIC	Participa identificando riesgos en los sistemas informáticos que usa						
	Participación en proyectos tecnológicos	Tienen en cuenta su opinión para la automatización en proyectos tecnológicos de la empresa						
	Participación en la ejecución de pruebas de control	Participa en pruebas/certificación de los sistemas informáticos a implementar		1=Totalmente en desacuerdo				
Planificación de los sistemas de información (VD)	Control al sistema de información	En la planificación de proyectos, hay supervisión los puntos correspondientes a TIC	2=En desacuerdo					
	Control de recursos de infraestructura tecnológica	Cree que la empresa planifica y ejerce control de los recursos de infraestructura tecnológica	3=Ni de acuerdo ni en desacuerdo					
	Control de recursos de software	Cree que la empresa planifica y ejerce control de los recursos de software	4=De acuerdo					
	Metodología de implementación	Considera que hay una metodología para la implementación de sistemas de información	5=Totalmente de acuerdo					
	Estrategia de SI	Cree que los SI son producto del análisis de proyectos tecnológicos a fin de apoyar las estrategias de la empresa						
Desempeño de mecanismos de seguridad de la información (VI)	Control y procedimientos de acceso al SI	Se encuentra satisfecho con los SI de su área, percibe un adecuado control						
	Segregación de funciones en el SI	Según su área considera alta la concentración de funciones de los SI de su área						
	Políticas de seguridad y acceso al sistema	Existen políticas y normas implementadas que mejoran el desempeño del sistema y de los usuarios						

*TIC = Tecnologías de la información

*SI = Sistema de información

*VD = Variable dependiente

*VI = Variable independiente

ANEXO 09 CUESTIONARIO

Con la finalidad de obtener un panorama claro acerca de los sistemas de información y sus mecanismos de seguridad, se tiene el siguiente cuestionario. Cabe resaltar que los resultados se utilizarán con fines académicos, de carácter anónimo y confidencial.
A continuación, se muestran una serie de afirmaciones. Estas han sido elaboradas de forma que permitan indicar hasta qué punto está de acuerdo con ellas. Favor de marcar acorde a su opinión cualquiera de las cinco alternativas, siguiendo la escala de Likert.

1. TD : Totalmente en desacuerdo.
2. D : En desacuerdo.
3. N : Neutral, ni de acuerdo ni desacuerdo.
4. A : De acuerdo.
5. TA : Totalmente de acuerdo

Nº	PREGUNTAS	ALTERNATIVA				
		TD	D	N	A	TA
1	Participa en capacitaciones acerca del uso de los sistemas informáticos de su área					
2	Tienen en cuenta su opinión para el diseño de los sistemas de seguridad informática de su empresa					
3	Participa identificando riesgos en los sistemas informáticos que usa					
4	Tienen en cuenta su opinión para la automatización en proyectos tecnológicos de la empresa					
5	Participa en pruebas/ certificación de los sistemas informáticos a implementar					
6	En la planificación de proyectos, hay supervisión los puntos correspondientes a TIC					
7	Cree que la empresa planifica y ejerce control de los recursos de infraestructura tecnológica					
8	Cree que la empresa planifica y ejerce control de los recursos de software					
9	Considera que hay una metodología para la implementación de sistemas de información					
10	Cree que los SI son producto del análisis de proyectos tecnológicos a fin de apoyar las estrategias de la empresa					
11	Se encuentra satisfecho con los SI de su área, percibe un adecuado control					
12	Según su área considera alta la concentración de funciones de los SI de su área					
13	Existen políticas y normas implementadas que mejoran el desempeño del sistema y de los usuarios					

**ANEXO 10
RESULTADOS CODIFICADOS**

**RESULTADOS CODIFICADOS PARA LA VARIABLE DEPENDIENTE:
PARTICIPACION DEL USUARIO**

PRE PRUEBA					
PREGUNTA	P1	P2	P3	P4	P5
DIGITAL	68	64	57	67	42
FISICO	157	166	178	161	166
PROMEDIO	2,20588235	2,25490196	2,30392157	2,23529412	2,03921569
PROMEDIO	2,206	2,255	2,304	2,235	2,039
POS PRUEBA					
PREGUNTA	P1	P2	P3	P4	P5
DIGITAL	94	97	88	82	89
FISICO	337	325	326	331	329
PROMEDIO	4,2254902	4,1372549	4,05882353	4,04901961	4,09803922
PROMEDIO	4,225	4,137	4,059	4,049	4,098

**RESULTADOS CODIFICADOS PARA LA VARIABLE DEPENDIENTE:
PLANIFICACIÓN DE SISTEMAS**

PRE PRUEBA					
PREGUNTA	P6	P7	P8	P9	P10
DIGITAL	56	82	66	63	71
FISICO	151	156	173	162	168
PROMEDIO	2,02941176	2,33333333	2,34313725	2,20588235	2,34313725
PROMEDIO	2,029	2,333	2,343	2,206	2,343
POS PRUEBA					
PREGUNTA	P6	P7	P8	P9	P10
DIGITAL	84	94	95	90	96
FISICO	336	344	339	347	346
PROMEDIO	4,11764706	4,29411765	4,25490196	4,28431373	4,33333333
PROMEDIO	4,118	4,294	4,255	4,284	4,333

**RESULTADOS CODIFICADOS PARA LA VARIABLE INDEPENDIENTE: DESEMPEÑO
DE MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN**

PRE PRUEBA			
PREGUNTA	P6	P7	P8
DIGITAL	79	75	52
FISICO	159	157	151
PROMEDIO	2,33333333	2,2745098	1,99019608
PROMEDIO	2,333	2,275	1,99
POS PRUEBA			
PREGUNTA	P6	P7	P8
DIGITAL	94	103	101
FISICO	341	342	338
PROMEDIO	4,26470588	4,3627451	4,30392157
PROMEDIO	4,265	4,363	4,304