



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS
Y DE COMERCIO**

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA



**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN FINANZAS–CONTADOR PÚBLICO-AUDITOR**

AUTORAS:

**FERNANDA GISSELA GÁLVEZ ESCOBAR
JOSELINE MARIELA SÁNCHEZ CAJAMARCA**

**DIRECTOR:
ECON. FRANCISCO CAICEDO**

**LATACUNGA
2018**

*Empieza haciendo lo necesario,
después lo posible, y de repente
te encontrarás haciendo lo imposible.*

San Francisco de Asís



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

TEMA:

“ANÁLISIS DEL COSTO-BENEFICIO EN LAS EMPRESAS DEL SECTOR INDUSTRIAL REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍAS QUE UTILIZAN HERRAMIENTAS DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA PROVINCIA DE COTOPAXI, DURANTE EL PERÍODO 2012-2016”



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

- Diseño de una antena y reloj inteligente
- Automóvil Eléctrico



Espionaje en la Industria Tecnológica



Generan virus y códigos maliciosos

- Sus Estratégias evitan interrupciones en sus servicios



- 24%, ocasionando engaños y ataques a los sistemas de las industrias

Phishing, Delitos Informáticos



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

FORMULACIÓN DEL PROBLEMA

¿Deficiente inversión en herramientas de seguridad y protección de información conlleva a pérdidas económicas?



JUSTIFICACIÓN

Usuarios externos lograr tener acceso y llegar hasta la información protegida



Controles los aplican de manera correcta

Investigar herramientas, para minimizar el riesgo de robo

Sector industrial estratégico.
Buen funcionamiento



OBJETIVOS

Objetivo General

Analizar el costo-beneficio de las Herramientas de Seguridad y Protección de Datos en las empresas del Sector Industrial reguladas por la Superintendencia de Compañías en la Provincia de Cotopaxi en el período 2012 - 2016.



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Objetivos Específicos

Determinar las empresas del sector industrial reguladas por la Superintendencia de Compañías que trabajan bajo el enfoque de buenas prácticas tales como ISO, 27001, 27002, o la Ley Ecuatoriana y la perspectiva gerencial hacia la inversión en herramientas de seguridad y protección de Datos

Realizar un levantamiento de información sobre el costo de las Herramientas de Seguridad y Protección de Datos que podrían utilizar las empresas del sector industrial.

Determinar el beneficio marginal de la inversión que genera a las empresas del sector industrial reguladas por la Superintendencia de Compañías en la provincia de Cotopaxi al utilizar herramientas de seguridad y protección de datos.

Construir un catálogo de inversiones en Herramientas de Seguridad y Protección de Datos para las empresas del Sector Industrial reguladas por la Superintendencia de Compañías.



Capítulo II

Marco Referencial

- Resguardo
- Integridad
- Confidencialidad

Seguridad de
la Información



- Información es un activo fundamental para el desarrollo de un Negocio

ISO 27001



- Políticas
- Recursos Humanos
- Activos
- Accesos
- Incidentes

ISO 27002



- Decisión sobre qué alternativa es preferida.

Inversión



- Retorno sobre la Inversión en Seguridad

ROSI



- Posibilidad de ocurrencia de una amenaza provocan debilidades

Vulnerabilidad



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Sistema de Variables

V.D.



Incremento del beneficio dentro de las organizaciones del sector industrial reguladas por la Superintendencia de Compañías en Seguridad y Protección de datos.

V.I.

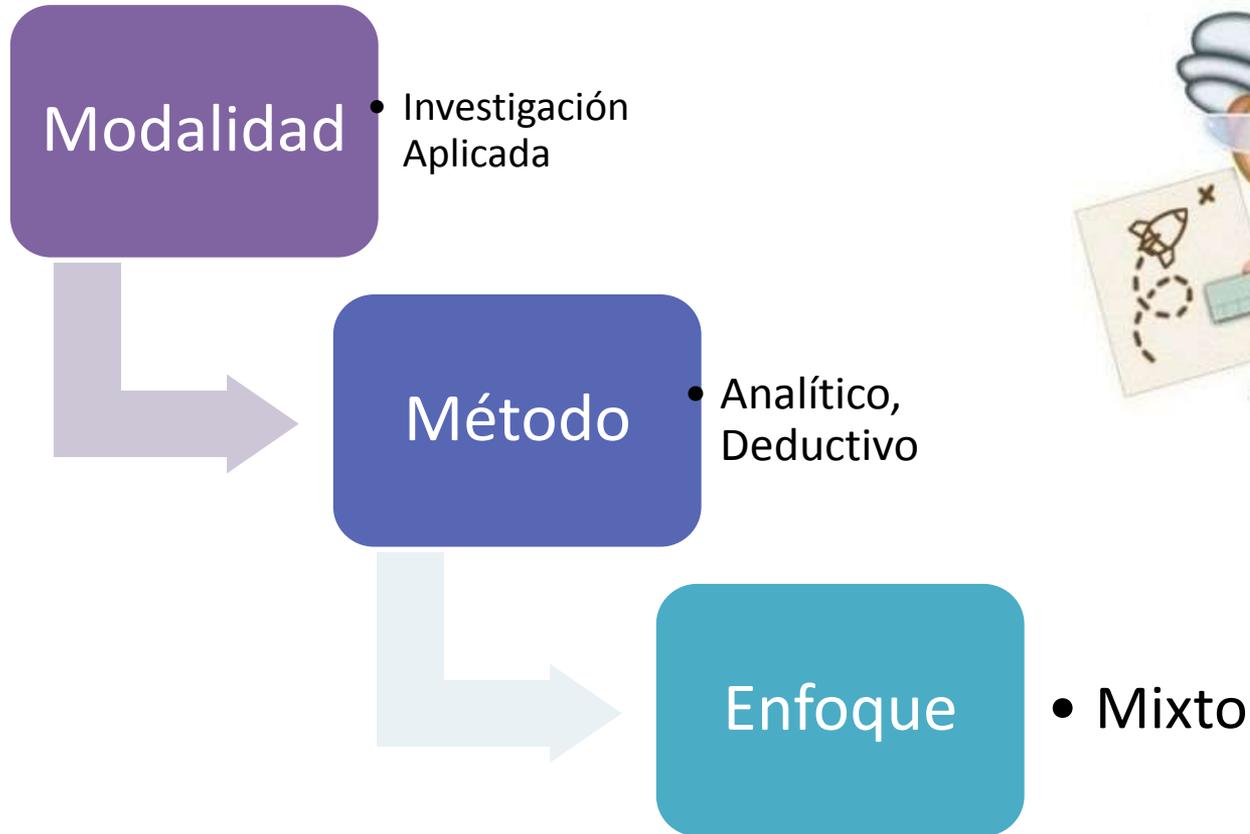


Inversión en la aplicación de Herramientas de Seguridad de Información en las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.



Capítulo III

Metodología de la Investigación



Muestra

Muestreo Intencional por cuotas

EMPRESAS DEL SECTOR INDUSTRIAL				
REGULADAS DE LAS POR LA SUPER INTENDECNIA DE COMPAÑÍAS, VALORES Y SEGUROS				
N°	NOMBRE DE LA EMPRESA	TAMAÑO	AÑO 2016	
			EQUIPO DE COMPUTO	INGRESOS POR VENTAS
1	NOVACERO S.A	GRANDE	\$ 101.810,20	\$ 201.736.885,00
2	AGLOMERADOS COTOPAXI SOCIEDAD ANONIMA	GRANDE	\$ 847.522,57	\$ 44.420.457,45
3	CORPORACION ECUATORIANA DE ALUMINIO SA CEDAL	GRANDE	\$ 638.071,29	\$ 58.756.867,51
4	MOLINOS POULTIER SA	GRANDE	\$ 184.294,05	\$ 20.600.747,68
5	PASTEURIZADORA EL RANCHITO CIA. LTDA	GRANDE	\$ 77.487,31	\$ 16.870.182,20
6	PRODICEREAL S.A.	GRANDE	\$ 13.721,58	\$ 12.675.345,46
7	PARMALAT	GRANDE	\$ 114.719,36	\$ 27.743.707,57
8	FAMILIA SANCELA	GRANDE	\$ 2.064.542,26	\$ 155.812.434,00
9	PROVEFRUT	GRANDE	\$ 217.106,00	\$ 57.148.555,00
10	INDUSTRIA DE LICORES ECUATORIANOS LICOREC S.A.	MEDIANA	\$ 97.709,50	\$ 2.696.298,98
11	DLIP INDUSTRIAL DLIPINDUSTRIAL S.A.	MEDIANA	\$ 15.501,48	\$ 1.090.752,06
12	INDUACERO INDUSTRIA DE ACERO DEL ECUADOR CIA. LTDA.	MEDIANA	\$ 16.159,67	\$ 2.574.062,67
13	FUENTES SAN FELIPE S.A. SANLIC	MEDIANA	\$ 68.555,72	\$ 1.667.149,80
14	CONSTRUCCIONES ULLOA CIA. LTDA.	MEDIANA	\$ 2.065,00	\$ 1.351.798,28
15	CARNIDEM CIA. LTDA.	MEDIANA	\$ 16.758,01	\$ 2.575.274,12
16	LA FINCA CIA. LTDA.	MEDIANA	\$ 1.759,18	\$ 3.425.998,26
17	PRODUCTORA Y COMERCIALIZADORA DE LOS HELADOS DE SALCEDO CORPICECREAM S.A.	PEQUEÑA	\$ 12.731,43	\$ 787.827,81
18	CALZACUBA CIA. LTDA.	PEQUEÑA		\$ 366.741,26
19	EDITORIAL LA GACETA S.A.	PEQUEÑA	\$ 25.440,85	\$ 392.948,27
20	MOLINOS OROBLANCO CIA. LTDA.	PEQUEÑA	\$ 1.187,36	\$ 767.696,42
21	PROCESADORA DE NEUMÁTICOS COTOPAXI PRONEUMACOSA S.A.	PEQUEÑA	\$ 0,00	\$ 389.805,65
22	ANDES KINKUNA S.A.	MICROEMPRESA	\$ 6.329,57	\$ 80.020,52

Fuente: (Superintendencia de Compañías Valores y Seguros del Ecuador, 2017)

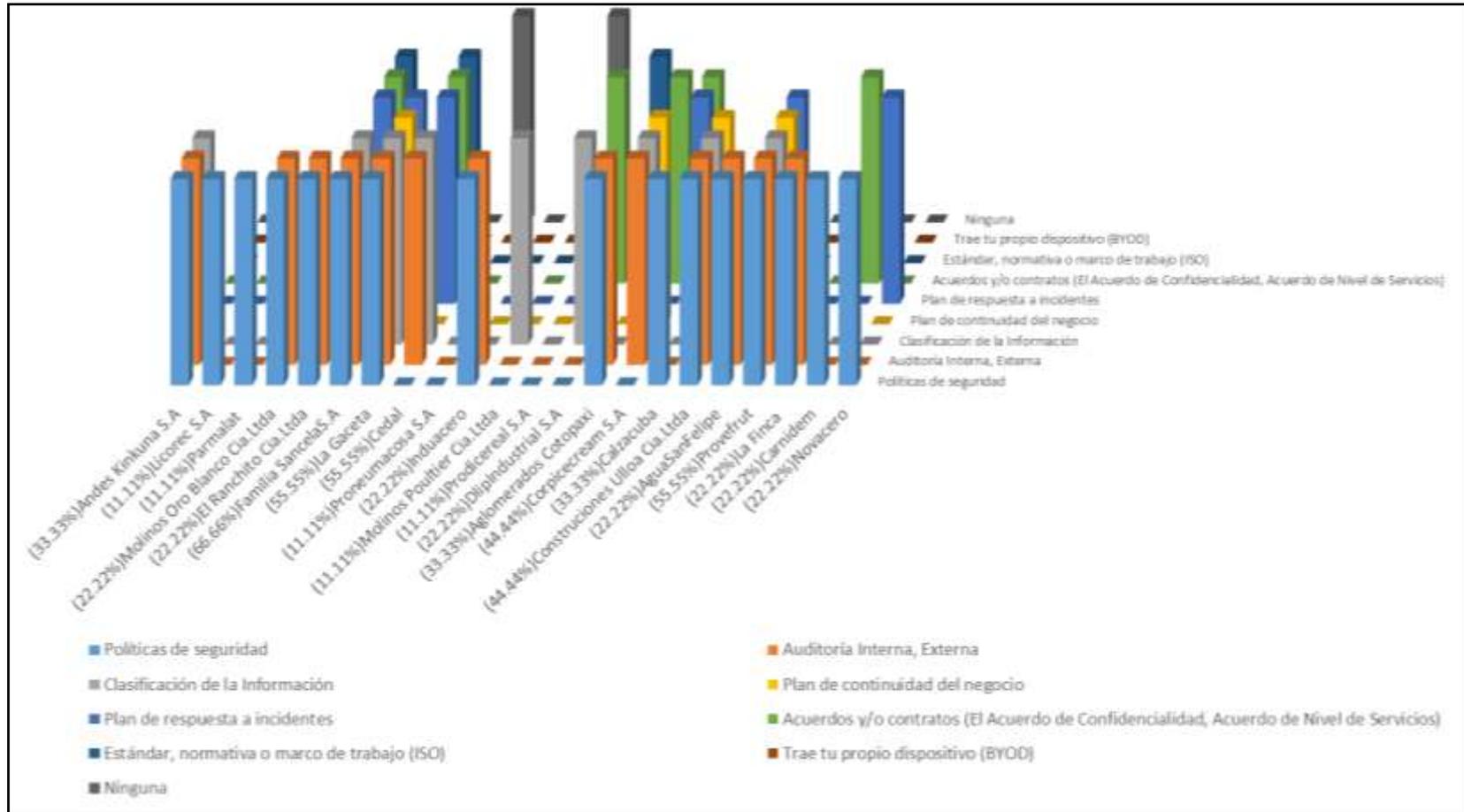


Capítulo IV

Resultados de la Investigación

¿Cuáles son las prácticas de Gestión de Sistemas de información que la empresa ha implementado durante los años 2012-2016?

Administración

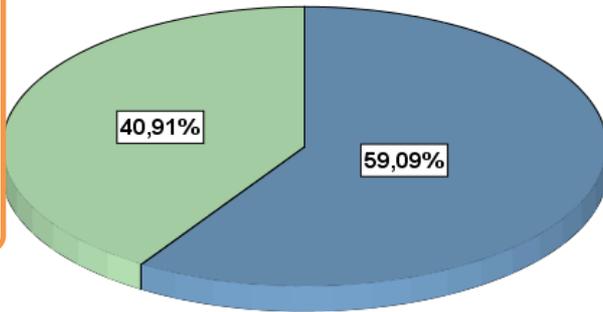


¿Los empleados de la organización reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas de seguridad de información y procedimientos para seguridad de la información?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	13	59,1	59,1
NO	9	40,9	100,0
Total	22	100,0	

7. ¿Los empleados de la organización reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas de seguridad de información y procedimientos para seguridad de la información?

■ SI
■ NO

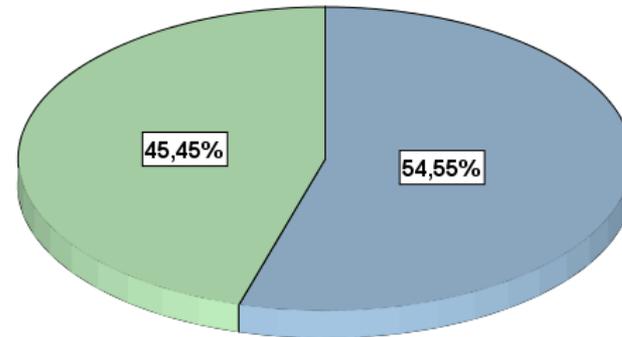


¿Los usuarios autorizados a utilizar los accesos a redes y los servicios de red cuentan con políticas de control de Accesos a la información?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	12	54,5	54,5
NO	10	45,5	100,0
Total	22	100,0	

12. ¿Los usuarios autorizados a utilizar los accesos a redes y los servicios de red cuentan con políticas de control de Accesos a la información?

■ SI
■ NO



Tecnología de la Información

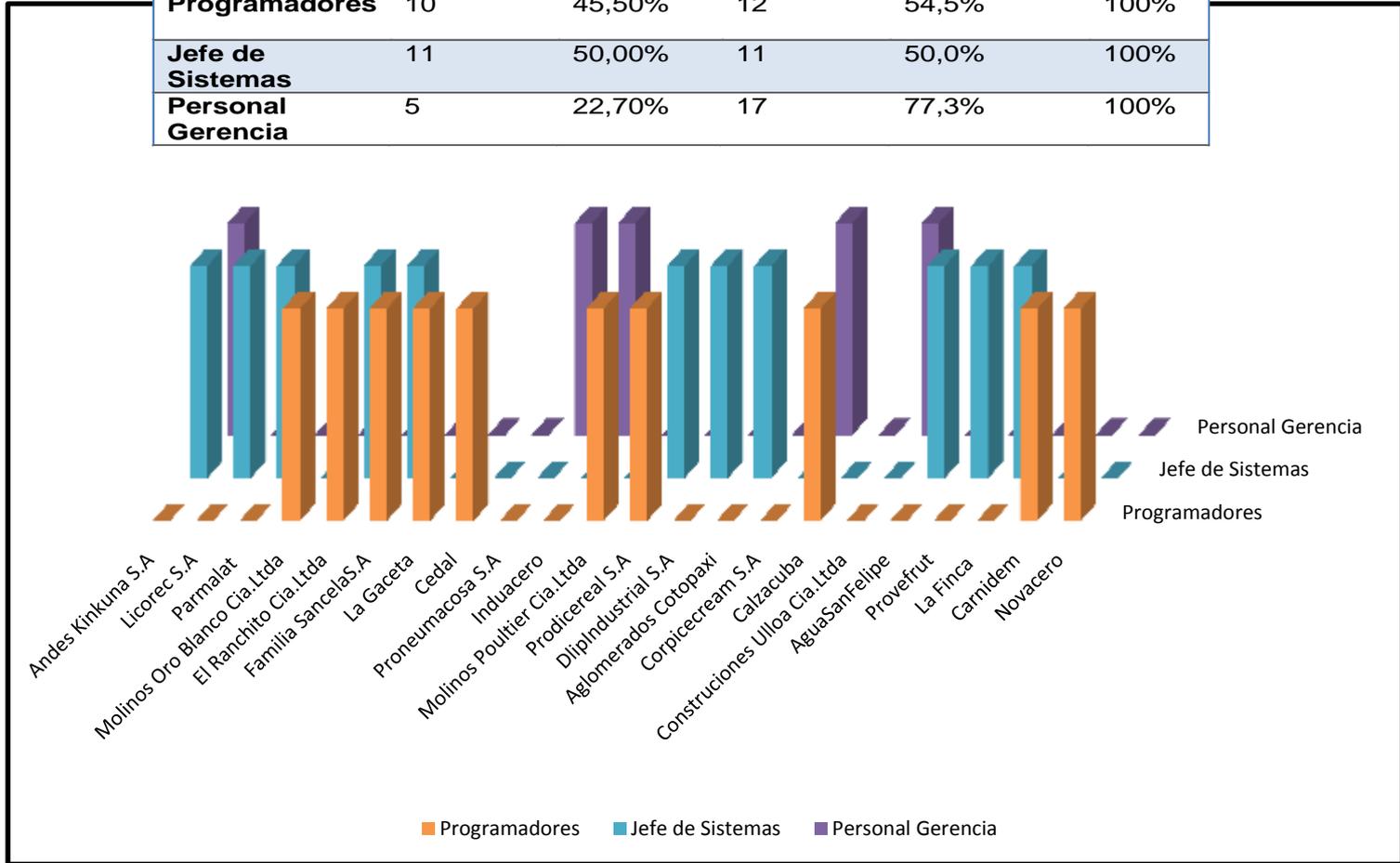
Administración



¿Qué tipo de empleados tienen acceso al código fuente de las aplicaciones de software?

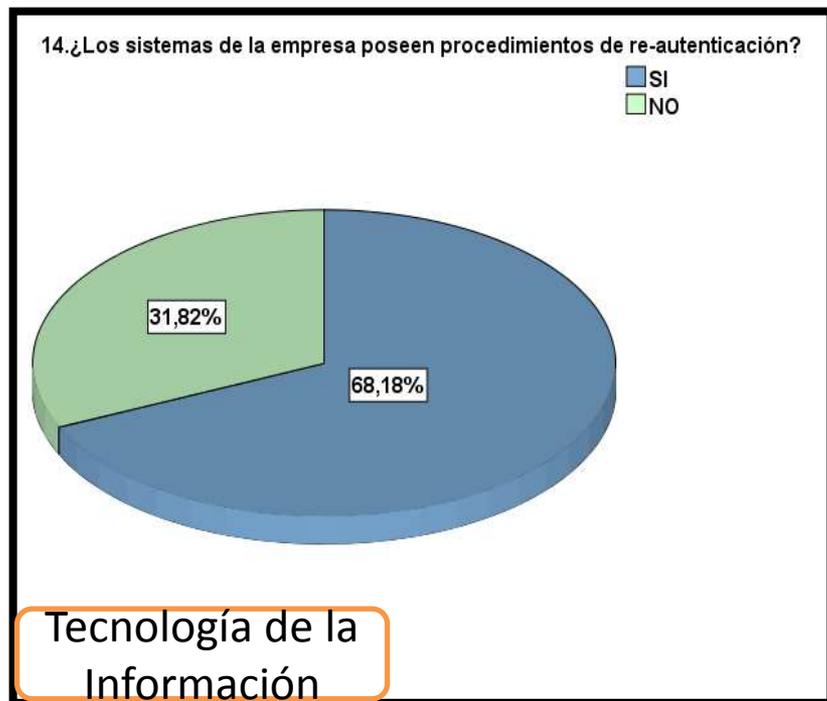
Personal	INCLUYE		NO INCLUYE		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
Programadores	10	45,50%	12	54,5%	100%
Jefe de Sistemas	11	50,00%	11	50,0%	100%
Personal Gerencia	5	22,70%	17	77,3%	100%

Tecnología de la Información



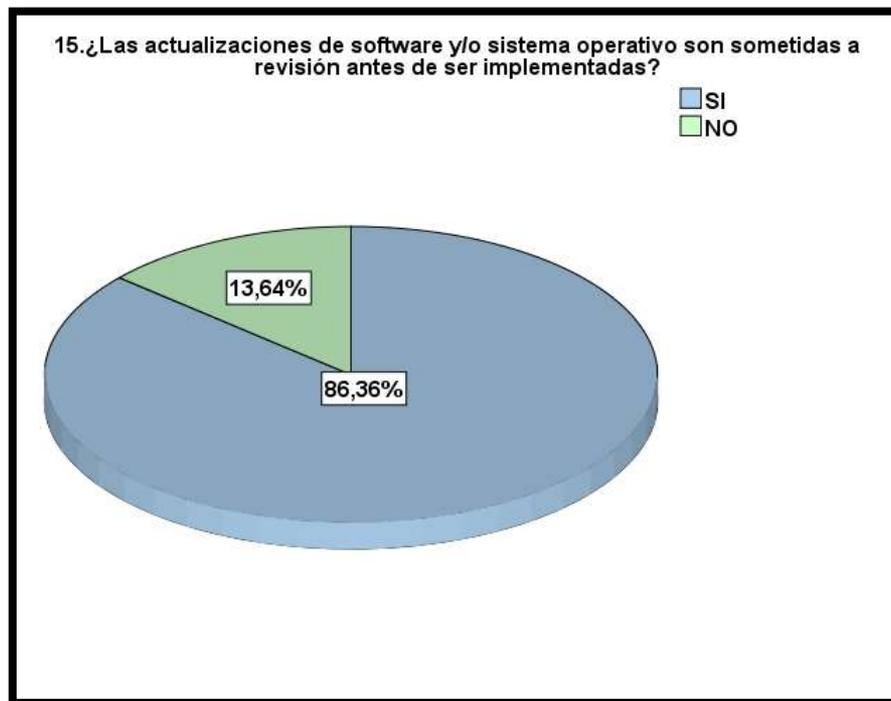
¿Los sistemas de la empresa poseen procedimientos de re-autenticación?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	15	68,2	68,2
NO	7	31,8	100,0
Total	22	100,0	



¿Las actualizaciones de software y/o sistema operativo son sometidas a revisión antes de ser implementadas?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	19	86,4	86,4
NO	3	13,6	100,0
Total	22	100,0	



¿Se administra y controla las redes para acceso solo de equipos autorizados?

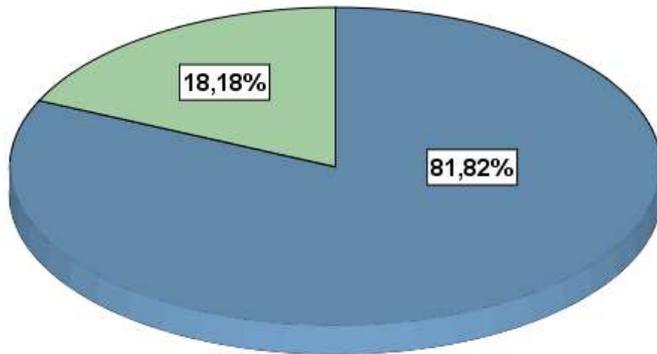
Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	18	81,8	81,8
NO	4	18,2	100,0
Total	22	100,0	

¿La empresa cuenta con controles criptográficos?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	10	45,5	45,5
NO	12	54,5	100,0
Total	22	100,0	

20. ¿Se administra y controla las redes para acceso solo de equipos autorizados?

■ SI
■ NO



Tecnología de la Información

25. ¿La empresa cuenta con controles criptográficos?

■ SI
■ NO

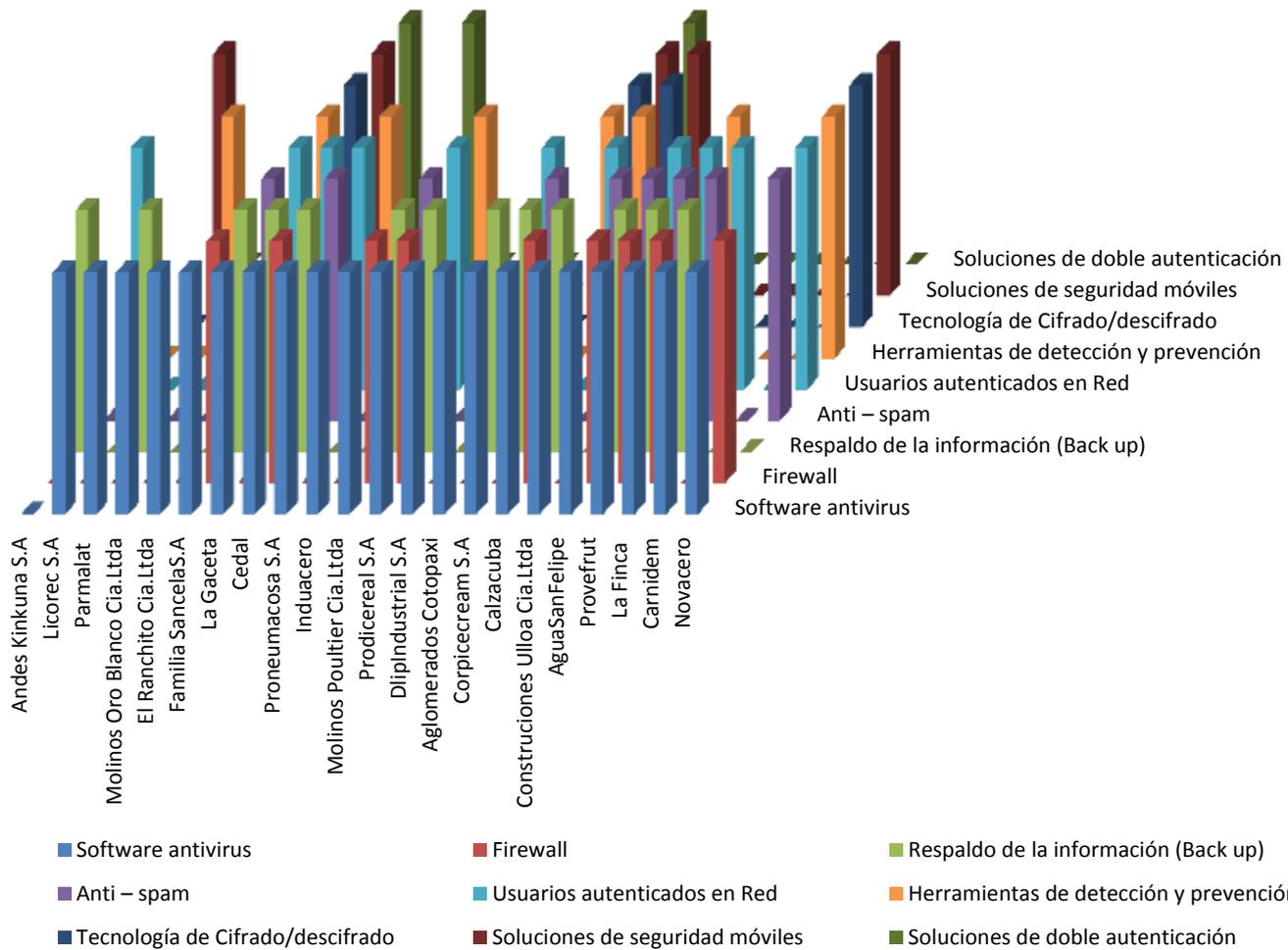


¿Cuáles de los siguientes controles de seguridad se ha implementado en su empresa para protección de información?

Control	INCLUYE		NO INCLUYE		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
Software antivirus	21	95,5%	1	4,5%	100%
Firewall	9	40,9%	13	59,1%	100%
Respaldo de la información (Back up)	13	59,1%	9	40,9%	100%
Anti – spam	9	40,9%	13	59,1%	100%
Usuarios autenticados en Red	11	50,0%	11	50,0%	100%
Herramientas de detección y prevención	8	36,4%	14	63,6%	100%
Tecnología de Cifrado/descifrado	4	18,2%	18	81,8%	100%
Soluciones de seguridad móviles	5	22,7%	17	77,3%	100%
Soluciones de doble autenticación	3	13,6%	19	86,4%	100%

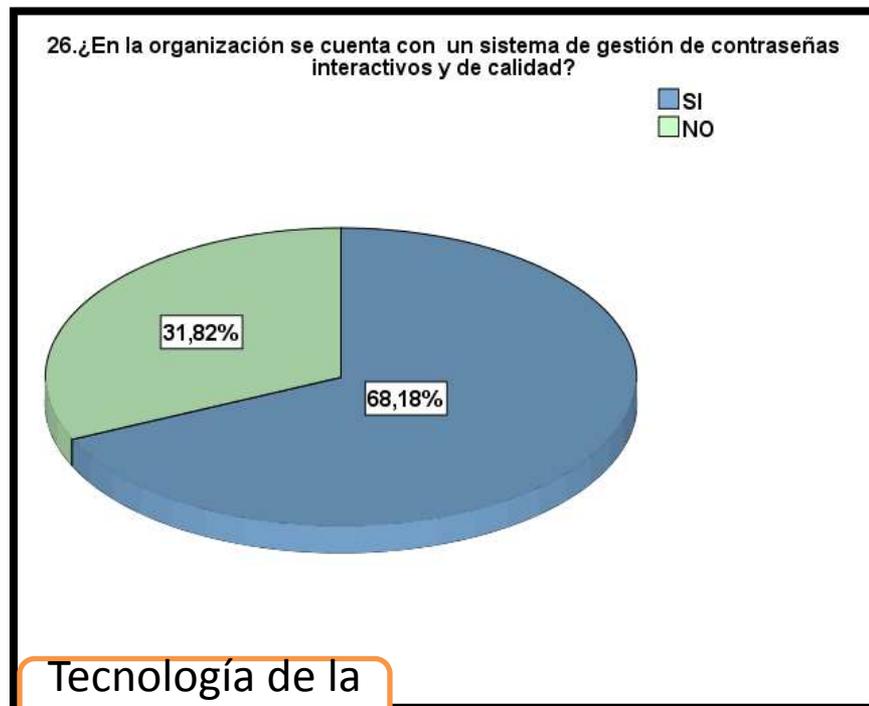


22. ¿Cuáles de los siguientes controles de seguridad se ha implementado en su empresa para protección de información?



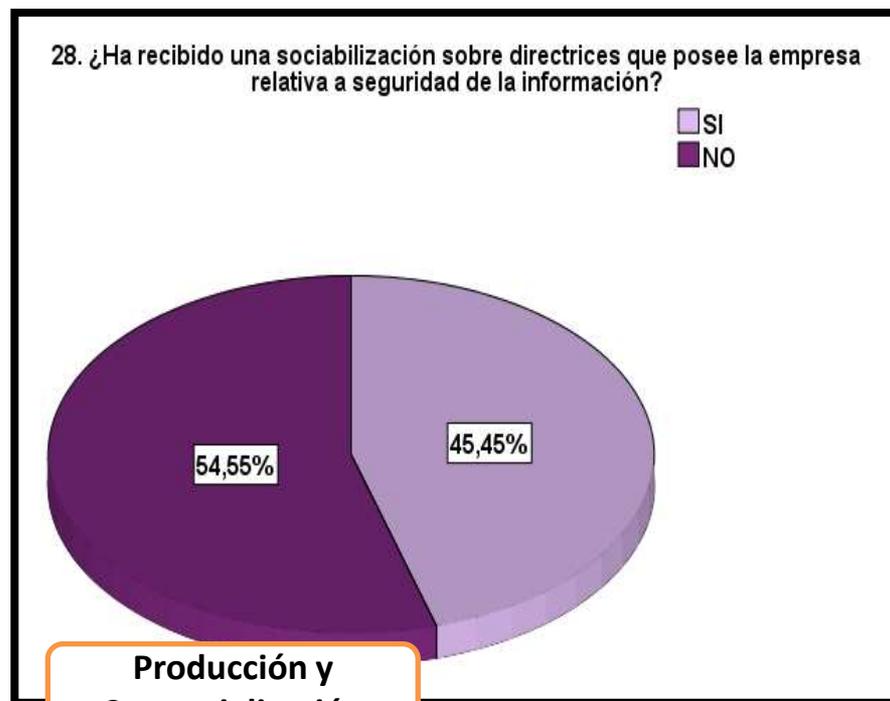
¿En la organización se cuenta con un sistema de gestión de contraseñas interactivos y de calidad?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	15	68,2	68,2
NO	7	31,8	100,0
Total	22	100,0	



¿Ha recibido una sociabilización sobre directrices que posee la empresa relativa a seguridad de la información?

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	10	45,5	45,5
NO	12	54,5	100,0
Total	22	100,0	



Tecnología de la Información

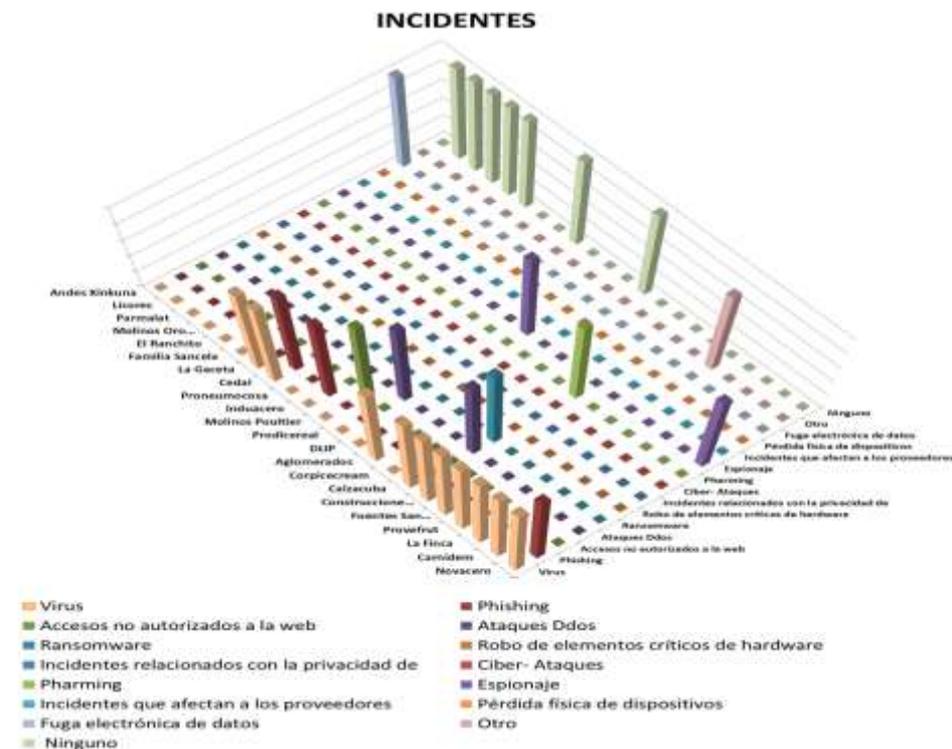
Producción y Comercialización



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

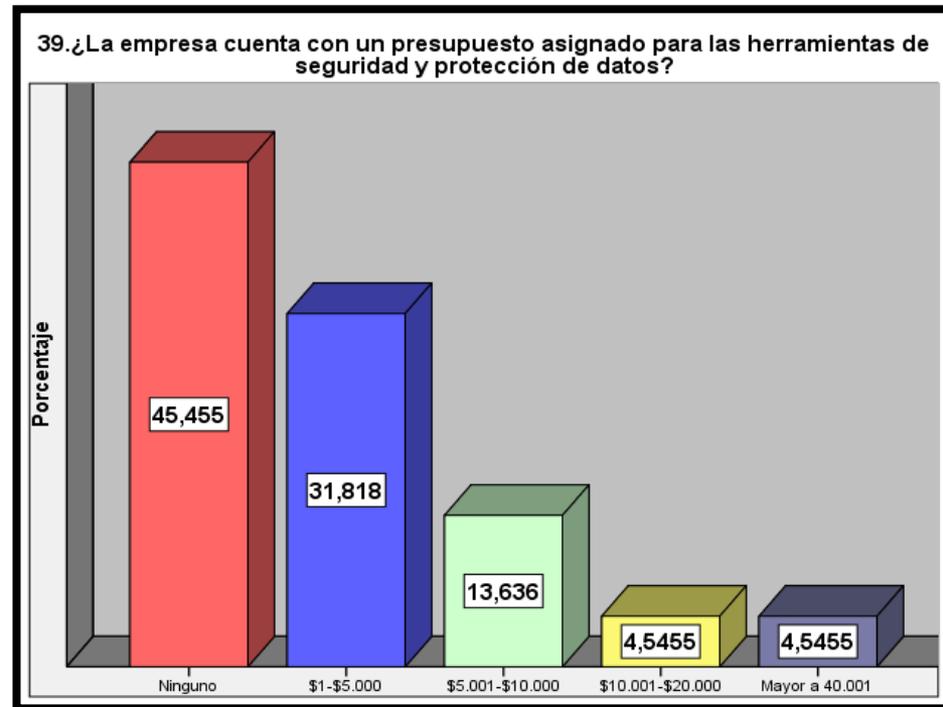
Seleccione los tipos de incidentes de seguridad de información que sufrió la empresa durante el período 2012-2016.

Incidentes	Sufrieron Respuestas		No sufrieron Respuestas		TOTAL
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	
Virus	10	45,45%	12	54,54%	100,0%
Phishing	3	13,63%	19	86,36%	100,0%
Accesos no autorizados a la web	1	4,54%	21	95,45%	100,0%
Ataques Ddos	2	9,09%	20	90,90%	100,0%
Ransomware	1	4,54%	21	95,45%	100,0%
Pharming	1	4,54%	21	95,45%	100,0%
Espionaje	2	9,09%	20	90,90%	100,0%
Fuga electrónica de datos	1	4,54%	21	95,45%	100,0%
Otro	1	4,54%	21	95,45%	100,0%
Ninguno	7	31,81%			



¿La empresa cuenta con un presupuesto asignado para las herramientas de seguridad y protección de datos?

Presupuesto	Frecuencia	Porcentaje	Porcentaje acumulado
Ninguno	10	45,5	45,5
\$1-\$5.000	7	31,8	77,3
\$5.001-\$10.000	3	13,6	90,9
\$10.001-\$20.000	1	4,5	95,5
Mayor a 40.001	1	4,5	100,0
Total	22	100,0	



COMPROBACIÓN DE HIPÓTESIS

HIPÓTESIS

H_1

La inversión en herramientas de seguridad y protección de datos genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

H_0

La inversión en herramientas de seguridad y protección de datos no genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.



COMPROBACIÓN DE HIPÓTESIS

37. ¿Tiene herramientas adecuadas para el resguardo de la información?			Respuestas		Total
			SI	NO	
2. ¿Cuánto aproximadamente ha invertido la empresa en el período 2012-2016 en herramientas de seguridad y protección de datos?	Ninguno	Recuento	0	1	1
		Frecuencia esperada	,9	,1	1,0
	\$1-\$5000	Recuento	5	1	6
		Frecuencia esperada	5,5	,5	6,0
	\$5001-\$10000	Recuento	4	0	4
		Frecuencia esperada	3,6	,4	4,0
	\$10001-\$20000	Recuento	6	0	6
		Frecuencia esperada	5,5	,5	6,0
	\$20001-\$40000	Recuento	2	0	2
		Frecuencia esperada	1,8	,2	2,0
	Mayor a \$40001	Recuento	3	0	3
		Frecuencia esperada	2,7	,3	3,0
	Total	Recuento	20	2	22
		Frecuencia esperada	20,0	2,0	22,0

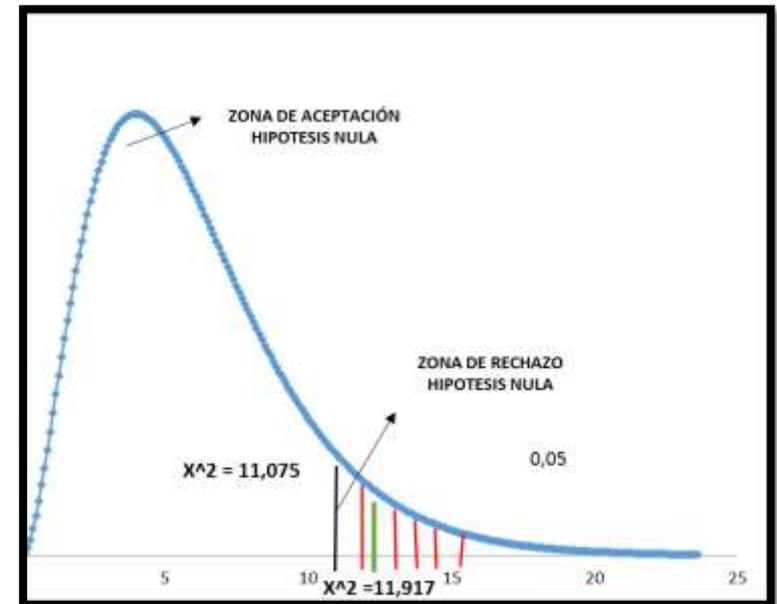


COMPROBACIÓN DE HIPÓTESIS

Pruebas de Chi-cuadrado			
	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	11,917a	5	,036
Razón de verosimilitudes	7,997	5	,156
Asociación lineal por lineal	4,062	1	,044
N de casos válidos	22		

v/p	0,001	0,0025	0,005	0,01	0,025	0,05
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705

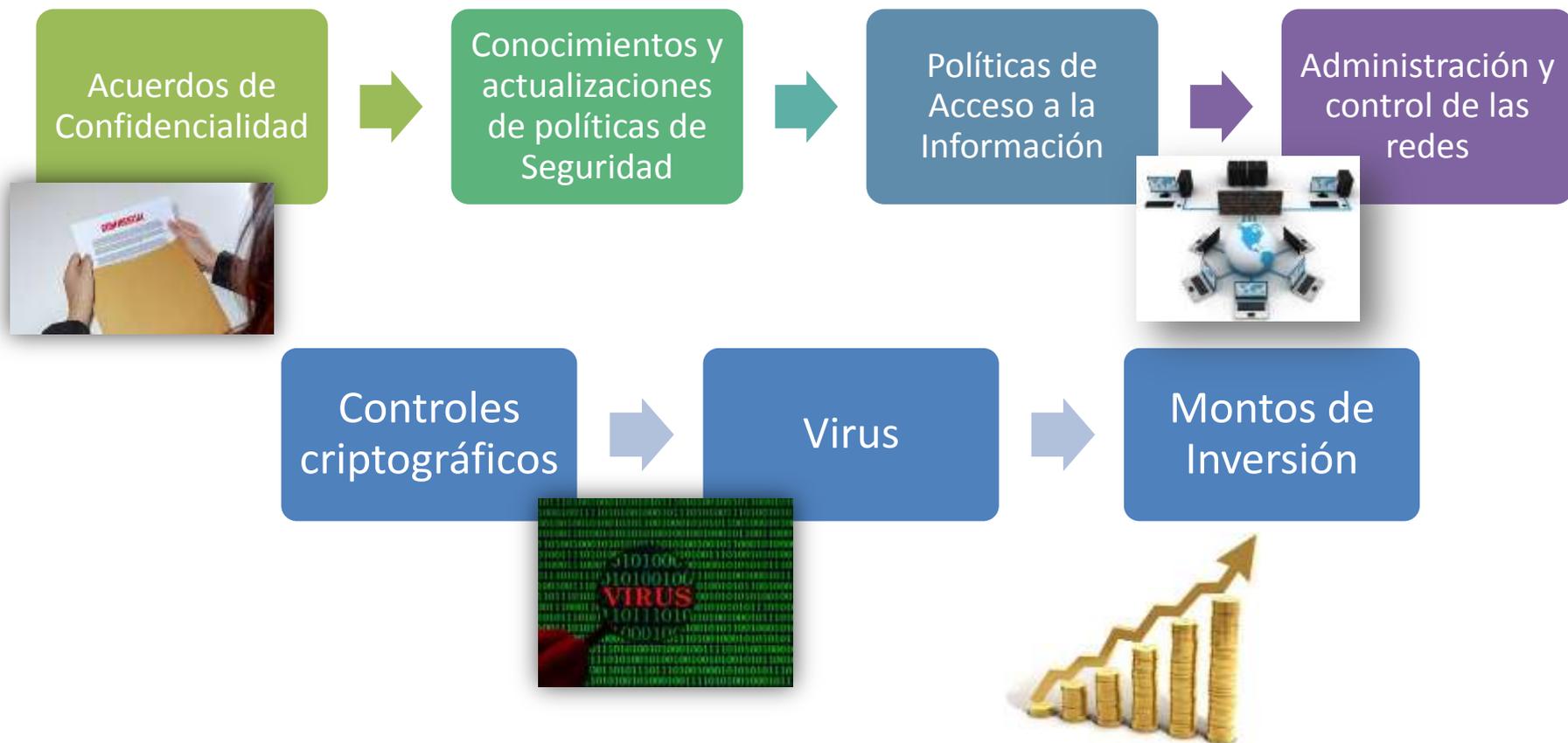
Grados de Libertad $(\#C-1)(\#F-1)$
 $= (2-1)(6-1) = 1 * 5 = 5$



CAPÍTULO V

ANÁLISIS COSTO BENEFICIO

Caso 1: Debilidades



Políticas

- Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.
- Uso adecuado de correo electrónico
- Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales
- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.





Herramientas necesarias a ser implementadas

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	\$400
Políticas de accesos a la información	Solución Uno Equipo servidor/Configuración proxy ACL	\$2.000/\$700
Administración y control de las redes	Un rack	\$400
	Router	\$500
	Switch	\$150
	Pach Panel	\$70
	Configuraciones	\$300
Controles criptográficos	Instalación y Configuraciones	\$235
Presupuesto corrección de fallas		\$4.755

Las empresas que necesitan respaldo de información (BAKUP)	\$200 Anuales
Licencias Antivirus 15 maquinas	\$600 Anuales
Capacitaciones	\$300
Total Presupuesto de Inversión	\$1.100 Anuales



RETORNO DE LA INVERSIÓN EN SEGURIDAD INFORMÁTICA ROSI

ROSI= (Exposición del Riesgo, % Riesgo mitigado) – Costo de la Solución

Datos:

Costo promedio de los incidentes.

\$12500

% Riesgo mitigado

90%

Costo promedio de los costos de inversión

\$4100

$$\text{ROSI} = (12500 * 90\%) - 4100$$

$$\text{ROSI} = 11.250 - 4100$$

$$\text{ROSI} = 7.150$$

$$\text{Relación} = 7.150 / 4100$$

$$\text{Relación} = 174\%$$



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Conclusiones

Las empresas que se analizó del sector industrial reguladas por la Superintendencia de Compañías mediante las encuestas realizadas presentaron, qué mayor parte de las entidades no cuentan con la certificación de la Norma ISO (International Standardization Organization) 27001:2013, de igual manera la perspectiva de Gerencia hacia el cumplimiento de la misma presenta niveles bajos en temas de Gestión en sistemas de información, a más de ello se constató que las empresas tratan de cumplir con varios controles de acuerdo a la ISO 27002:2013 misma que es una ayuda para el cumplimiento de la certificación ISO 27001:2013.

Dentro de las empresas que se tomó como referencia para la investigación presenta un 45,5% (porcentaje tomado de las encuestas) no tienen presupuesto designado para hardware, software, soporte informático, capacitaciones del conocimiento de las políticas en seguridad informática.



Conclusiones

De acuerdo al estudio de campo realizado a las empresas del sector Industrial se obtuvo que el 27,3% de las industrias poseen planes de respuesta a incidentes como prácticas de sistemas de información durante los periodos 2012-2016 y el 72,7% no cuentan con estos planes.

Según los resultados obtenidos de las preguntas dirigidas a los gerentes de las empresas del Sector Industrial se obtuvo que en el 40,9% no se da un entrenamiento apropiado del conocimiento y actualizaciones de las políticas de seguridad de información.

De acuerdo a los resultados obtenidos del ROSI en promedio el retorno de la inversión en seguridad de la información es de 174%, es decir que al invertir \$4.100 se logra una disminución del nivel del riesgo de \$7.150, para una mejor comprensión las empresas del sector Industrial por cada dólar que inviertan en seguridad de la información lograrán una disminución del riesgo de 1,74 dólares.



RECOMENDACIONES

Se recomienda a las empresas del Sector Industrial implementar un manual de políticas en seguridad información y protección de datos, basadas en los controles de la norma ISO 27002:2013, pues es uno de los parámetros para llevar a cabo la certificación ISO 27001:2013, ya que la misma es un beneficio al seguimiento y resguardo de la seguridad de la información en las empresas, así mismo es necesario que se realicen mejoras continuas en el transcurso de los años.

Se recomienda tomar como referencia y conocimiento de los costos aproximados para implementar los controles de acuerdo a la ISO 27002:2013, la misma que ayuda en la implementación de un buen Sistema en Seguridad, con la asistencia de hardware, sistemas de software, soporte informático, llevando a cabo una inversión inicial, un seguimiento continuo, ajustes necesarios en el transcurso de tiempo, que se puedan realizar y de esta forma las empresas puedan generar mejoras continuas en la Seguridad informática.



RECOMENDACIONES

Se recomienda a la administración de las empresas del Sector Industrial implementar planes de respuestas a incidentes, y de este modo estar preparados ante cualquier amenaza que pueda ocurrir y alterar el buen transcurso del negocio.

A los Jefes de Sistemas de las empresas del Sector Industrial programar capacitaciones referentes a las políticas corporativas de seguridad de información para el personal, además actualice sus conocimientos sobre la gestión de los sistemas de Información.

Se recomienda a la administración de las empresas del sector industrial realizar un análisis en cuestión de sistemas de seguridad de información y protección de datos, para que de esta manera se pueda tomar medidas apropiadas para evitar nuevas amenazas que puedan ir surgiendo en el transcurso del negocio.





Gracias



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA