UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR INDUSTRIAL DE LA PROVINCIA DE COTOPAXI.

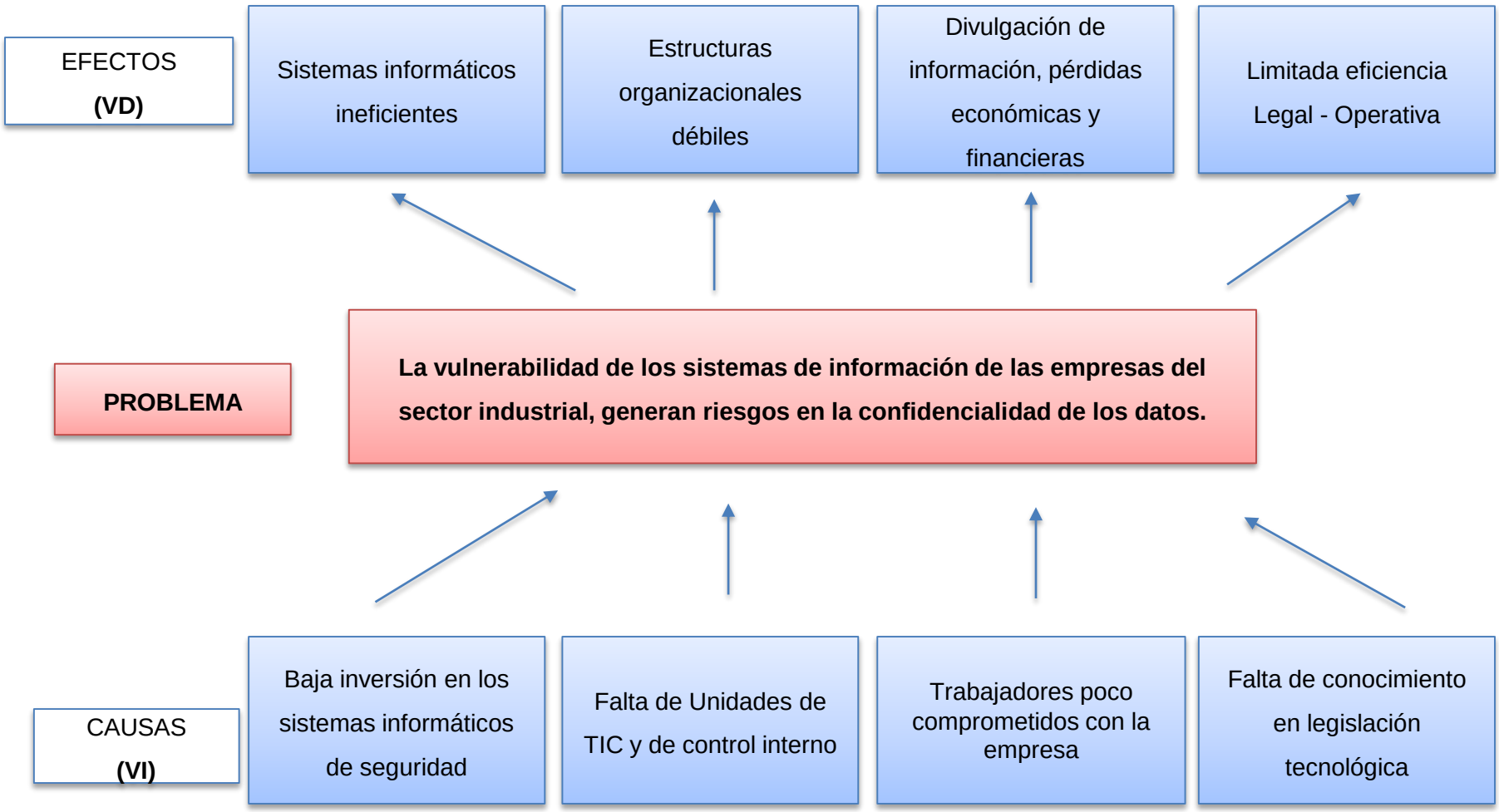
AUTORES: Diego Fernando Pinsha Defaz

Kleber Gonzalo Quevedo Zambonino

DIRECTOR: Ing. Luis Alfonso Lema Cerda

Latacunga, Diciembre 2017

ÁRBOL DE PROBLEMAS



JUSTIFICACIÓN

El estudio de fraudes informáticos debido a los cambios tecnológicos que se presentan día a día, lo cual incita a las organizaciones estar a la vanguardia de las ultimas herramientas con respecto a la protección de datos y seguridad de la información,

El crecimiento de ataques ha venido incrementándose a finales de 2016 e inicios de 2017 donde han surgido intromisiones de tipo ransomware, wannacry, bad rabbit, a visto necesaria la investigación en la protección de la información de las industrias

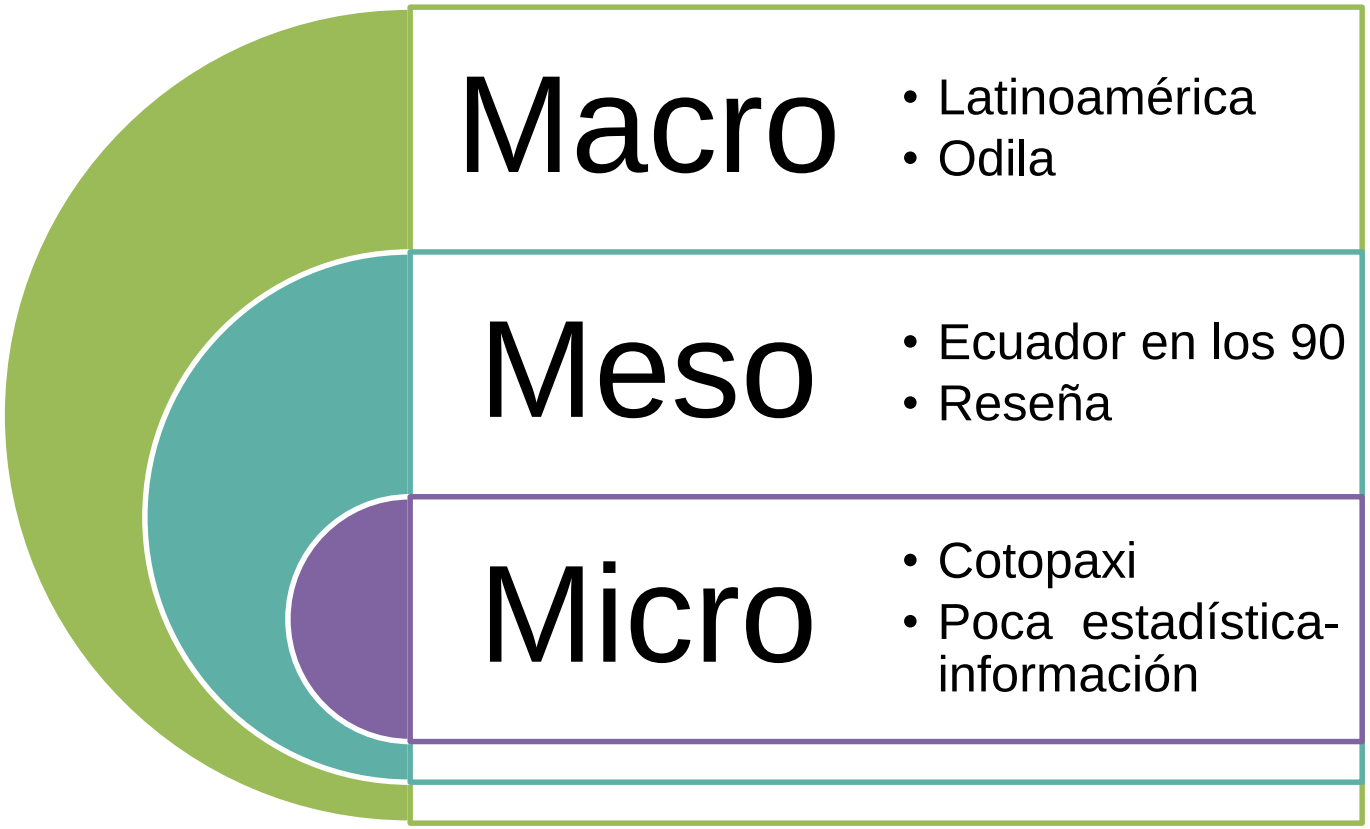
JUSTIFICACIÓN

Objetivo 11 del Plan Nacional del Buen Vivir

Política y Lineamiento(11.3)

- Fortalecer capacidades
- Impulsar el uso de las telecomunicaciones y TIC

PROBLEMÁTICA DE LA INVESTIGACIÓN



OBJETIVO GENERAL

- Analizar la vulnerabilidad a fraudes informáticos en las empresas del sector industrial mediante un examen especial que permita establecer parámetros de riesgo en la Provincia de Cotopaxi durante el periodo 2012 – 2016.

OBJETIVOS ESPECÍFICOS

- Describir la problemática de la investigación de acuerdo a las variables objeto de estudio para un mejor desarrollo de la misma.

- Definir las bases teóricas bajo las cuales se sustenta la investigación en torno a la vulnerabilidad de fraudes informáticos en las empresas industriales.

- Determinar los niveles de vulnerabilidad en fraudes informáticos para su posterior evaluación de las debilidades a nivel empresarial del sector industrial de la provincia de Cotopaxi.

OBJETIVOS ESPECÍFICOS

- Analizar los hallazgos, resultados y elaborar un informe de auditoría para determinar una opinión, tendencia de control en las empresas del sector industrial de la Provincia de Cotopaxi.
- Elaborar una Guía de Buenas Prácticas para el control de vulnerabilidades en Fraudes Informáticos para las empresas del sector industrial de la Provincia de Cotopaxi.

MARCO TEÓRICO

Empresas del Sector Industrial

Dedican a la transformación de materia prima en productos.

Actividades Principales (Cotopaxi)

METALMECÁNICA (Fabricación de tubos)
PRODUCTORA DE PAPEL
MADERERA
METALMECÁNICA (Fundición, refinación)
ELABORACION DE ALIMENTOS Y BEBIDAS

CIIU (Clasificación Industrial Internacional Uniforme) (C)

CIIU	Actividad
15	Elaboración de productos y bebidas
18	Fabricación de prendas de vestir y teñido de piel
19	Curtido y adobo de cueros, fabricación de maletas, bolsos a mano
20	Producción de madera y fabricación de productos de madera, corcho excepto muebles.
21	Fabricacion de papel y productos de papel
25	Fabricación de productos de caucho y plástico
27	Fabricación de metales comunes
28	Fabricación de productos de metal excepto maquinaria y equipo

MARCO TEÓRICO

Tecnologías de Información y Comunicación (TIC)

- Son un factor de vital importancia en la transformación de la economía global y en los ligeros cambios que se presenta en el mundo entero.

Fraude Informático

- El fraude Informático es conocido como un acto deliberado e ilegitimo que causa perjuicio patrimonial a una persona provocando un beneficio económico al cibercriminal o a una tercera persona

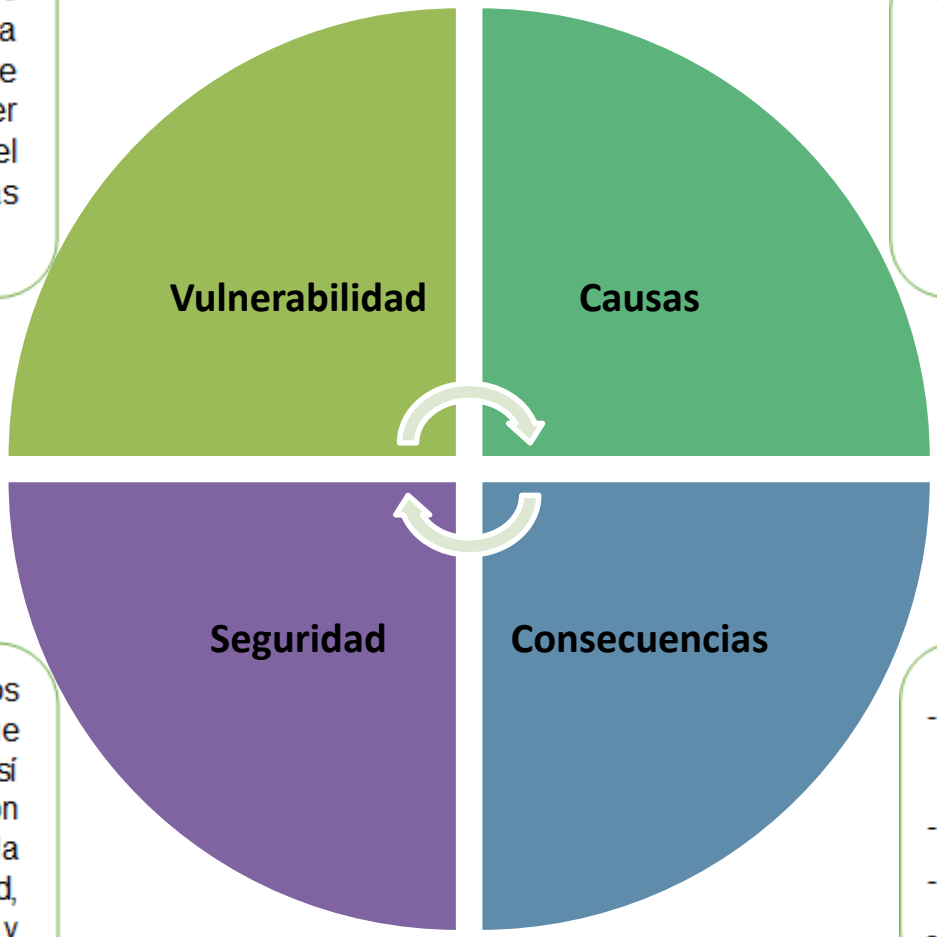
Tipos de Fraudes

- Fraude IP-PBX
- Phishing
- Open Proxy
- BotNet
- Fraudes en redes sociales

* Encriptación de la información
* Correos maliciosos
* Virus
* Borrado de datos
* Suplantación de identidad

MARCO TEÓRICO

- Se dan por el acceso no autorizado, errores y la destrucción de datos que pueden ocurrir en cualquier momento ya sea en el software y hardware de las empresas.



- Existencia de puertas traseras en el software.
- Descuido de los fabricantes en las aplicaciones.

- Medidas preventivas en los sistemas tecnológicos que permitan resguardar; así como proteger la información buscando mantener la confidencialidad, integridad, disponibilidad, autenticación y el no repudio (CIDAN).

- Complejidad en el manejo de la información.
- Programación errónea.
- Perdida de información.
- Filtración de datos ocultos.

MARCO TEÓRICO

COSO

BASE LEGAL

CÓDIGO ORGÁNICO INTEGRAL PENAL

Art.190.- Apropiación Fraudulenta por medios electrónicos. (Pena 1 a 3años)
Art.229.- Revelación ilegal de la base de datos. (Pena 1 a 3 años)
Art.232.- Ataques a la integridad de los sistemas informáticos. (Pena 3 a 5 años)
Art.234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. (Pena 3 a 5 años)

POBLACIÓN

Dentro de la población considerada para el estudio se tomaron en cuenta a todas las empresas del sector industrial de la Provincia, que dentro de sus estados financieros cuentan con saldos de inversión en la cuenta **Equipo de computo**, según la información obtenida en la Superintendencia de Compañías.

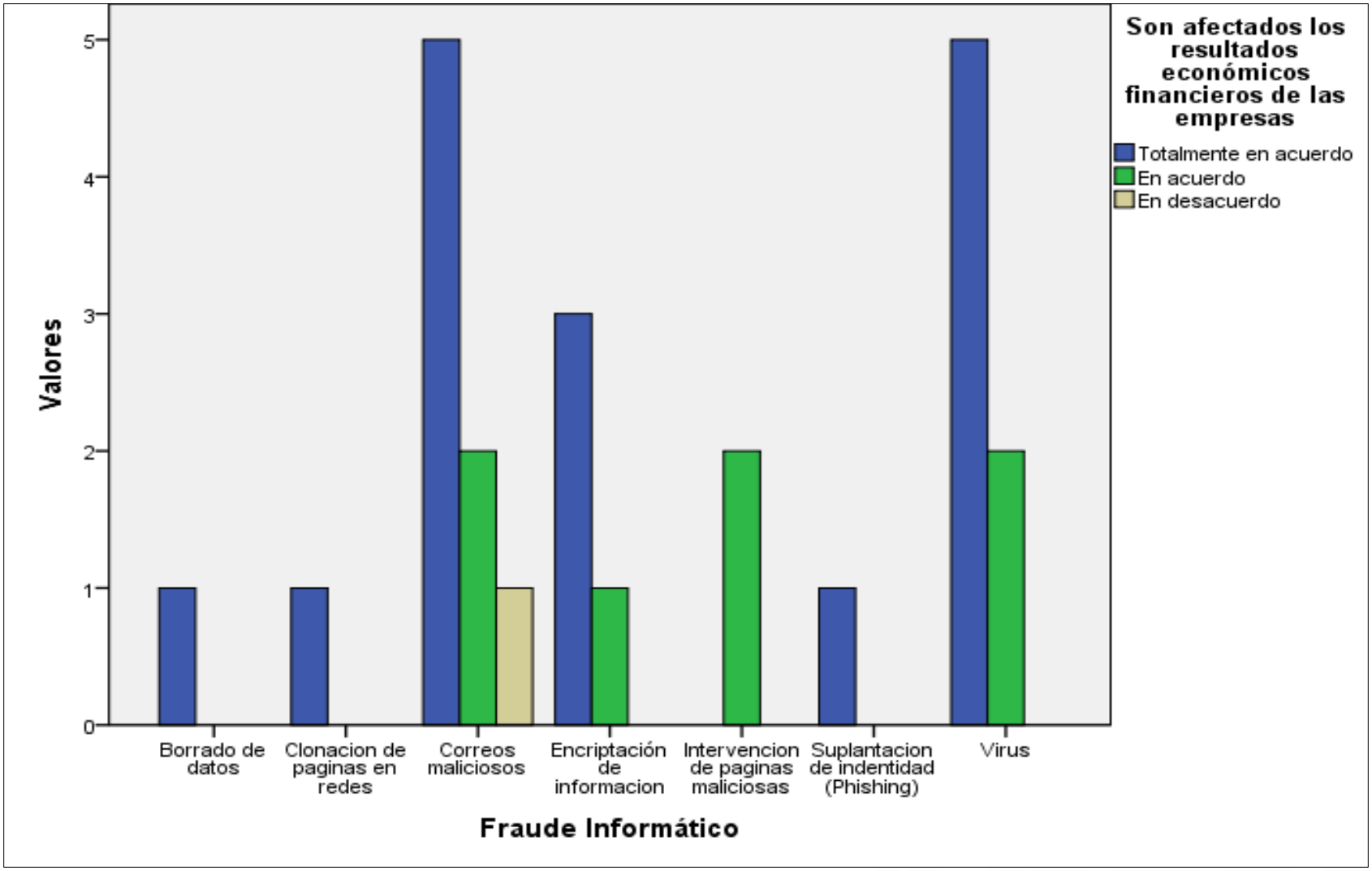
MUESTRA

La muestra es calculada de manera intencional de acuerdo a un proceso de diagnostico financiero, en lo cual se toma a todas las empresas que tengan un porcentaje de inversión mas representativa en el total de propiedad planta y equipo con un total de 20 empresas evaluadas.

MUESTRA

N°	Denominación	Edificios y Otros Inmuebles Costo Histórico	Maq. Equipo y Otras Insta. Costo Histórico	Muebles y Enseres	Otras PP&E	Equipo Computo	TOTAL	% Inversión
1	CARNIDEM CIA. LTDA.	$ 97.500,00	$ 810.266,44	$ 7.596,20	$ 0,00	**$ 16.758,01**	$ 932.120,65	**1,80%**
2	LICOREC S.A.	$ 230.808,89	$ 959.749,23	$ 42.522,89	$ 214.841,33	**$ 97.493,21**	$ 1.545.415,55	**6,31%**
3	IMP.ADRIAN IMCEAL	$ 0,00	$ 2.292,37	$ 6.040,51	$ 0,00	**$ 4.737,75**	$ 13.070,63	**36,25%**
4	DLIP INDUSTRIALS.A.	$ 219.000,00	$ 1.314.842,48	$ 13.661,28	$ 3.916,48	**$ 15.501,48**	$ 1.566.921,72	**0,99%**
5	MOLINOS POULTIER S.A.	$ 587.338,44	$ 2.569.992,31	$ 33.860,34	$ 0,00	**$ 183.064,20**	$ 3.374.255,29	**5,43%**
6	INDUACERO CIA. LTDA.	$ 508.888,58	$ 664.474,91	$ 11.793,86	$ 0,00	**$ 16.159,67**	$ 1.201.317,02	**1,35%**
7	CONSTRUC. ULLOA	$ 0,00	$ 197.509,58	$ 0,00	$ 13.396,05	**$ 2.065,00**	$ 212.970,63	**0,97%**
8	EDITORIAL LA GACETA S.A.	$ 70.243,60	$ 35.000,00	$ 1.845,00	$ 3.480,32	**$ 25.440,85**	$ 136.009,77	**18,71%**
9	CALZACUBA CIA. LTDA.	$ 0,00	$ 25.241,13	$ 13.645,17	$ 0,00	**$ 7.260,74**	$ 46.147,04	**15,73%**
10	CEDAL S.A.	$ 5.501.819,58	$ 0,00	$ 109.492,84	$ 0,00	**$ 638.071,29**	$ 6.249.383,71	**10,21%**
11	FUENTES SAN FELIPE S.A.	$ 503.417,57	$ 350.073,32	$ 60.670,93	$ 21.040,55	**$ 68.555,72**	$ 1.003.758,09	**6,83%**
12	NOVACERO S.A.	$ 21.798.024,79	$ 91.555.522,89	$ 1.202.615,80	$ 1.014.822,40	**$ 1.120.705,28**	$ 116.691.691,16	**0,96%**
13	EL RANCHITO CIA. LTDA.	$ 1.586.412,57	$ 5.216.384,54	$ 29.561,89	$ 6.444,32	**$ 65.048,06**	$ 6.903.851,38	**0,94%**
14	PRODICEREAL S.A.	$ 681.748,44	$ 336.615,86	$ 53.407,77	$ 0,00	**$ 13.721,58**	$ 1.085.493,65	**1,26%**
15	AGLOMERADOS	$ 3.476.865,13	$ 22.282.083,53	$ 425.214,11	$ 0,00	**$ 847.522,57**	$ 27.031.685,34	**3,14%**
16	CORPICECREAM S.A.	$ 131.092,29	$ 208.211,53	$ 20.543,58	$ 0,00	**$ 12.731,43**	$ 372.578,83	**3,42%**
17	MOLINOS OROBLANCO	$ 0,00	$ 168.588,86	$ 1.840,08	$ 0,00	**$ 1.187,36**	$ 171.616,30	**0,69%**
18	PARMALAT DEL ECUADOR	$ 1.951.086,55	$ 7.123.863,81	$ 67.133,83	$ 0,00	**$ 114.719,36**	$ 9.256.803,55	**1,24%**
19	PROVEFUT S.A.	$ 3.349.088,16	$ 12.089.095,23	$ 15.987,30	$ 34.980,00	**$ 181.870,46**	$ 15.671.021,15	**1,16%**
20	FAMILIA SANCELA S.A.	$ 9.104.462,17	$ 40.580.996,81	$ 1.212.590,13	$ 0,00	**$ 2.064.542,26**	$ 52.962.591,37	**3,90%**

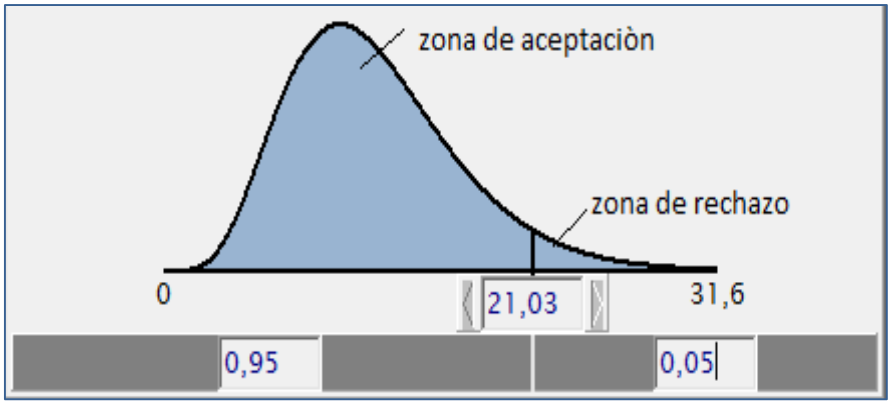
PRUEBA DE HIPOTESÍS



PRUEBA DE HIPOTESÍS

RESULTADOS

Con un nivel de confianza del 95% y con la probabilidad del 5% de cometer error, se obtiene 12 grados de libertad, obtiene los valores de 8,307 < 21,03 zona de aceptación, por tanto se rechaza la hipótesis alternativa y se acepta la hipótesis nula.



Chi-cuadrado de Pearson	8,307	12
Razón de verosimilitud	9,302	12
N° de casos válidos	**24**	

PRUEBA DE HIPOTESÍS

*Mediante la investigación de campo realizada (encuestas) y con la comprobación de chi-cuadrado en el estadístico SPSS se concluye que:

(H0) = Los fraudes informáticos no inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

SE ACEPTA

(H1) = Los fraudes informáticos inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

EVALUACIÓN CASO-EMPRESA CALZACUBA

Programa de Auditoria Informática
Departamento de tecnología de información y comunicación (TIC)

N°	Procedimientos	Referencia P/T	Elaborado por	Fecha
1	Verificar el monto de inversión en Tecnología de Información y Comunicación (TIC) por medio de los estados financieros de la empresa.	CS - 1/1	DFPD	14/08/2017
2	Solicitar al encargado del Departamento/Área de Tecnología de Información y Comunicación (TIC). la lista de equipos que se usen, cuantos usuarios la usan y cuantas horas al día son usados estos equipos	LE - 1/1	KGQZ	14/08/207
3	Elaboración de Cuestionarios de Control Interno al Departamento/Área de Tecnología de Información y Comunicación.	CCI - 1/3	KGQZ	15/08/207
4	Aplicación de Cuestionarios de Control Interno al Departamento/Área de Tecnología de Información y Comunicación (TIC).	CCI - 1/3 MCR -1/1	DFPD	16/08/207
5	Realizar un examen especial a los sistemas más vulnerables del Departamento/Área de Tecnología de Información y Comunicación (TIC).	EXE - 1/4	DFPD	16/08/207
6	Análisis Forense de los sistemas operativos dentro del área de TIC.	AF - 1/4	KGQZ	16/08/207
7	Elaboración de una hoja de Hallazgos de los resultados obtenidos.	HH - 1/3	KGQZ	18/08/207

Elaborado por: K.G.Q.Z. – D.F.P.D	Fecha: 14/08/2017
Revisado por : L.A.L.C	Fecha: 15/08/2017

EVALUACIÓN CASO-EMPRESA CALZACUBA

Resultados

Procedimiento 1

El monto de inversión en TIC de la empresa durante periodo de evaluación asciende a $ 27789,43.

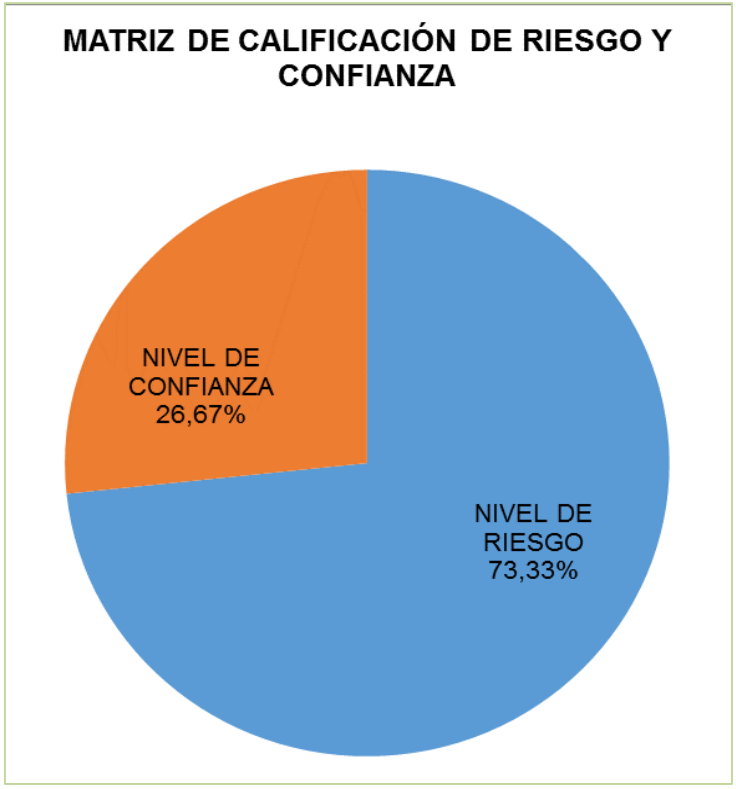
Procedimiento 2

Lista de Equipos					
Nº	Nombre del equipo de Computo	Responsable	Marque con una X		Hora de Uso
			Uso Único	Compartido	
1	Servidor		X		24
2	Computador HP	Marco Acuña		X	10
3	Computador SONY	Pamela Bautista	X		10
4	Computador LG	Jessy Moreno	X		10
5	Computador SAMSUNG	José Bautista	X		10
6	Impresora EPSON Matricial	Todos		X	10
7	Impresora EPSON	Todos		X	10
8	Teléfono Fijo PANASONIC	Todos		X	10
9	2 Cortapicos	Todos		X	10
Elaborado por: K.G.Q.Z. – D.F.P.D			Fecha: 14/08/2017		
Revisado por: L.A.L.C			Fecha: 15/08/2017		

EVALUACIÓN CASO-EMPRESA CALZACUBA

Procedimiento 3 Y 4

Se determinó que no existe un control eficiente en los sistemas de información desde la parte operativa de la empresa, lo que repercute inminentemente en posibles ataques informáticos generando múltiples afectaciones en la organización.



NR=(100-NC)			
CT	8	RIESGO	ENFOQUE
PT	30		
NC	26.67%	BAJO	
RC	73.33%	ALTO	CUMPLIMIENTO

EVALUACIÓN CASO-EMPRESA CALZACUBA CIA. LTDA.

Procedimiento 5

El examen especial se realizó debido a los hallazgos significativos encontrados durante la evaluación de control Interno, lo cual permitió evidenciar múltiples vulnerabilidades que tenían los sistemas de información.

El periodo de evaluación fue del 1 de enero del 2016 al 31 de julio del 2017, mediante la autorización del Ing. José Bautista Gerente general, y el Sr. Marco Acuña administrador de la empresa.

Debilidades hacia ataques cibernéticos e inseguridad en el manejo de los sistemas informáticos al no contar con un departamento de TIC, son deficientes los controles de spam, antivirus y protección de datos a través de un firewall u otros mecanismos de seguridad.

EVALUACIÓN CASO-EMPRESA CALZACUBA

Procedimiento 6

Análisis Forense Digital

Identificación del Ataque: Encriptación de la información.

Evidencia: Inicios del 2017, e inhabilitación de los sistemas, adopción de medidas de seguridad.

La información encriptada fue muy relevante, ascendiendo a un monto de 6000,00 dólares,

Preservación de la Evidencia: Los discos duros fueron reemplazados y estos se encuentran en ADS para la recuperación y obtención de la información que fue ocultada**.**

Análisis de la Evidencia: Esta información fue recabada de manera testimonial por parte del Gerente y el personal de la empresa.

EVALUACIÓN CASO-EMPRESA CALZACUBA

Procedimiento 7

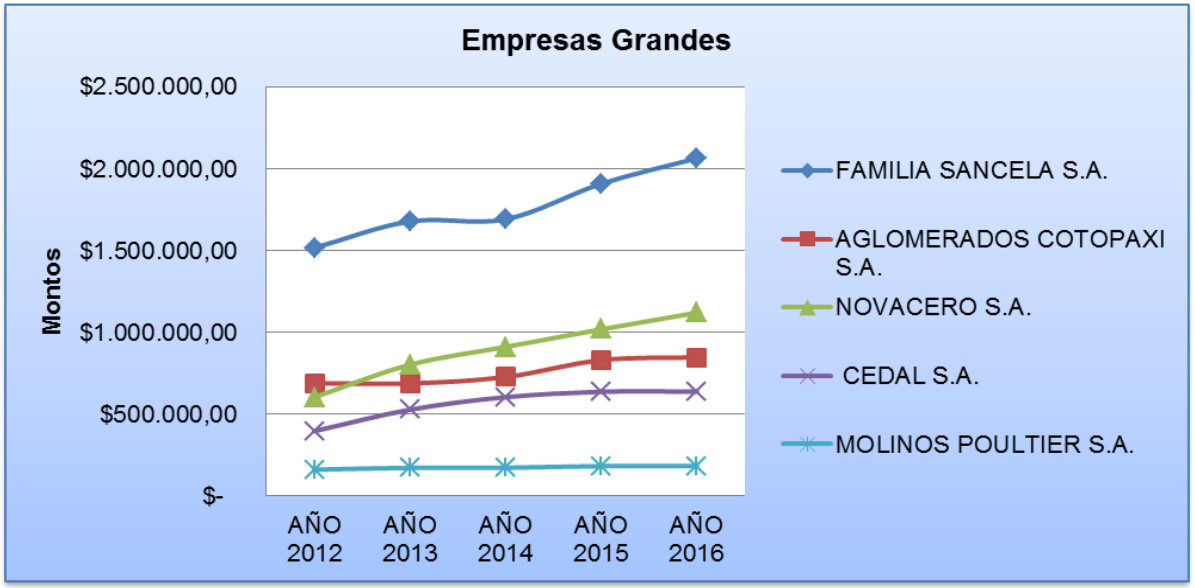
Hallazgos

Nombre del Hallazgo	Criterio	Causa	Efecto	Recomendación
Inexistencia de cámaras de video vigilancia	No posee con un manual de políticas y una guía de buenas prácticas para el uso de los sistemas informáticos.	El administrador de la empresa no considera necesario adaptar esta herramienta de seguridad.	La infraestructura de la empresa se encuentra vulnerable a posibles ataques cibernéticos.	Se recomienda al administrador de la empresa instalar cámaras de video vigilancia.
No posee un firewall	La empresa debe contar con software de protección de datos.	La empresa Calzacuba Cía. no posee un corta fuegos para bloquear a enlaces maliciosas.	La información de la puede ser vulnerada o sufrir ataques informáticos.	Se recomienda a la empresa implementar un firewall de seguridad.
No cuenta con notificaciones de acceso información.	La empresa debe activar mecanismos de defensa y protección en las herramientas de Office.	Los sistemas informáticos de la empresa, presentan puertos abiertos para ser atacados o vulnerados por hackers.	La empresa está inmersa a diversos fraudes informáticos.	Se recomienda al personal encargado de los ordenadores, activar comandos de protección de datos.
No cuenta con un Área de TIC.	La empresa debe contar con una área de TIC ya que ayuda de manera positiva a su desarrollo.	Por la falta de información y conocimiento del Gerente no cuenta con el área de TIC de manera formalizada.	Al no poseer el área de TIC el personal operativo utiliza de forma impropia la información de la empresa.	Se recomienda establecer un área de TIC dentro de la estructura organizacional de la empresa.
No existen informes del rendimiento de los sistemas.	La empresa debe contar con respaldos de informes del manejo de los sistemas de información.	La empresa que se encarga de la protección de datos no emite ningún reporte y que se estipulo dentro del contrato.	No se tiene reportes físicos que evidencien el adecuado rendimiento de los sistemas.	Se recomienda al administrador solicitar a la empresa ADS un reporte los sistemas.

TENDENCIA DE INVERSIÓN DE TIC EN LAS EMPRESAS DE LA PROVINCIA DE COTOPAXI

Grupo Nº 1

EMPRESAS INDUSTRIALES	AÑO 2012	AÑO 2013	AÑO 2014	AÑO 2015	AÑO 2016
FAMILIA SANCELA S.A.	$ 1.517.161,71	$ 1.678.753,33	$ 1.691.732,59	$ 1.908.739,98	$ 2.064.542,26
AGLOMERADOS COTOPAXI S.A.	$ 689.987,28	$ 688.072,15	$ 727.387,03	$ 830.868,94	$ 847.522,57
NOVACERO S.A.	$ 604.135,02	$ 802.620,57	$ 911.608,06	$ 1.018.895,08	$ 1.120.705,28
CEDAL S.A.	$ 397.106,04	$ 527.798,29	$ 604.077,93	$ 637.329,69	$ 638.071,29
MOLINOS POULTIER S.A.	$ 161.131,45	$ 172.011,05	$ 172.544,17	$ 183.064,20	$ 183.064,20

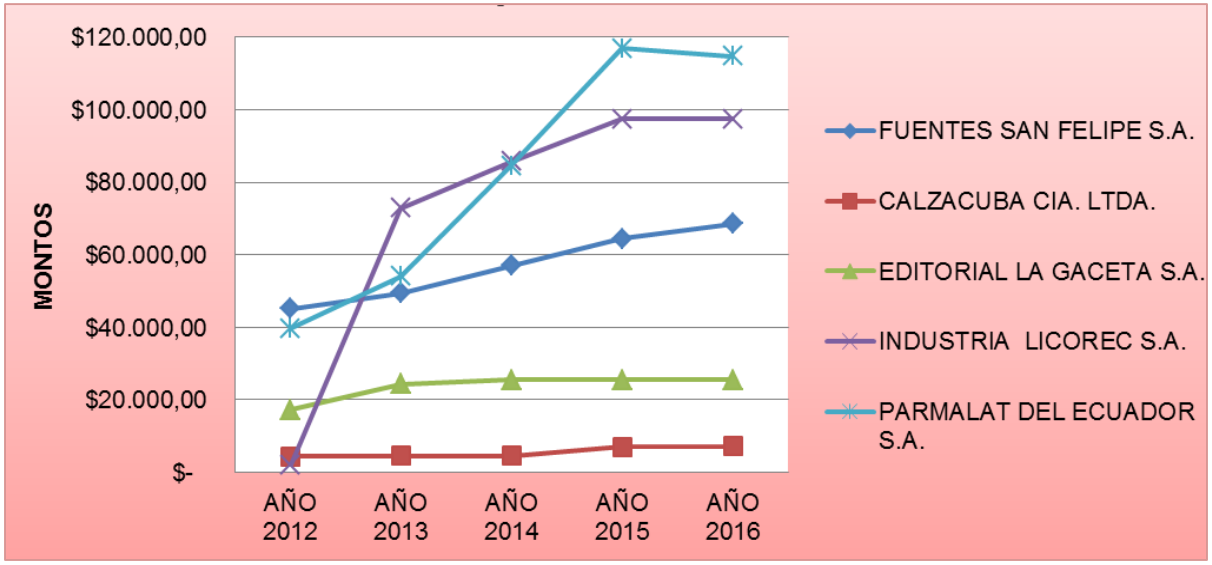


ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

TENDENCIA DE INVERSIÓN DE TIC EN LAS EMPRESAS DE LA PROVINCIA DE COTOPAXI

Grupo Nº 2

EMPRESAS INDUSTRIALES	AÑO 2012	AÑO 2013	AÑO 2014	AÑO 2015	AÑO 2016
FUENTES SAN FELIPE S.A.	$ 45.142,30	$ 49.429,68	$ 57.006,32	$ 64.499,32	$ 68.555,72
CALZACUBA CIA. LTDA.	$ 4.375,03	$ 4.571,46	$ 4.571,46	$ 7.010,74	$ 7.260,74
EDITORIAL LA GACETA S.A.	$ 17.245,85	$ 24.290,85	$ 25.440,85	$ 25.440,85	$ 25.440,85
INDUSTRIA LICOREC S.A.	$ 2.103,15	$ 72.898,82	$ 85.723,41	$ 97.493,21	$ 97.493,21
PARMALAT DEL ECUADOR S.A.	$ 39.596,71	$ 54.078,16	$ 84.582,16	$ 116.818,72	$ 114.719,36



PROPUESTA GUÌA DE BUENAS PRÁCTICAS EN TIC

Nuestra guía de buenas practicas para la protección y resguardo de la información de las diversas empresas cuenta con las siguientes secciones.

Sección	Temas
1	Fundamentos teóricos
2	Gestión de los activos
3	Medidas de seguridad básica
4	Seguridad de las operaciones
5	Herramientas de cifrado
6	Gestión del riesgo de TI
7	Detección de intrusos
8	Procesos, técnicas y normativa para la ciberseguridad dentro de las empresas
9	Nube de datos
10	Estudios, datos e información
11	Instrumento de evaluación
12	Representación gráfica de los diagramas de flujo

CONCLUSIONES

- Durante la investigación realizada lo primordial fue indagar a profundidad que tan vulnerables se encuentran las empresas del sector industrial a fraudes Informáticos, determinando que las pequeñas empresas son más propensas a ataques cibernéticos, esto se da debido a que las mismas no cuentan en su estructura organizacional con un departamento de tecnologías de información y comunicación que sirva de apoyo en el desarrollo de sus operaciones de manera sistemática y confiable.

- Para la ejecución de la presente investigación se inició con un diagnostico financiero obteniendo que del total de las empresas el 80% tienen una inversión significativa en propiedad planta y equipo en sus estados de situación financiera y de esta manera aplicar los instrumentos de recopilación de información en las entidades del sector manufacturero que se dedican a las siguientes actividades como es: construcción, metal mecánica, alimentos, bebidas, imprenta, calzado, lácteos, textiles y entre otros.

CONCLUSIONES

- Del estudio se determinó que la empresa Calzacuba fue víctima de Fraude Informático, por tanto mediante la aplicación de un cuestionario de Control Interno, herramienta de evaluación basada en los componentes del COSO, se demostró que las actividades de control; información y comunicación, tienen un nivel de confianza bajo de 26,67%, frente a un nivel de riesgo alto de 73,73% con respecto al ambiente de control, evaluación de riesgo, supervisión y monitoreo, constatando que no existe un control eficiente de los sistemas de información y por ende se deriva en una deficiente gestión en TIC.

- Para la comprobación de la hipótesis planteada se aplicó el test de Chi-Cuadrado donde se obtuvo un coeficiente de 8,31 zona de aceptación, por tanto se acepta la hipótesis nula se rechaza la hipótesis alternativa, estableciendo que los fraudes informáticos no inciden sustancialmente en los resultados económicos financieros de las empresas, ya que la mayoría de estas cuentan con sistemas de protección de datos e información eficientes y controlables, y la afectación se da en pequeñas y medianas empresas, debido a la falta de interés e inversión en recursos de tecnología de información.

CONCLUSIONES

- Se obtuvo la información necesaria con respecto a los fraudes informáticos más significativos que afectan a las empresas como son encriptación de información, borrado de datos, virus y correos maliciosos, siendo estos un foco de infección a los sistemas de información y datos sensibles, de la misma forma se pudo constatar que ciberdelincuentes atentan principalmente vía email como medio de intromisión.

- Se determina que existe una tendencia al alza con respecto a fraudes informáticos en las pequeñas y medianas empresas del sector industrial, debido a que no se invierte lo suficiente en la gestión de herramientas de TI, para satisfacer las necesidades de la empresa de manera integral con un método de evaluación integrado tanto individual como colectivamente acorde a las necesidades de la organización que ayuden en el respaldo de la información y protección de datos.

- Una vez finalizada la investigación a las empresas del sector industrial se pudo concluir que la mayoría no poseen un manual o guía de buenas prácticas con referente al manejo de las equipos de seguridad y protección de datos de información, con el propósito de facilitar el uso de herramientas de seguridad que permitan adoptar una buena gestión de riesgos de TIC.

RECOMENDACIONES

- Realizar más inversión en medios de protección de datos, aplicaciones y parches de seguridad con la finalidad de proteger intromisiones a los sistemas de información y comunicación de cada una de las áreas y departamentos; muy independiente de su actividad, logrando satisfacer las necesidades de ambas partes como son los trabajadores y los clientes creando un clima organizacional confiable.

- Estructurar planes estratégicos de TI acorde a los requerimientos del negocio de acuerdo al tamaño y a la actividad que se dediquen, ejecutando una buena gestión en la adopción de recursos de TI, lo cual permite a la organización ofrecer productos de calidad que satisfagan las necesidades de un mercado globalizado.

- A la comunidad científica, se propone ampliar los estudios de investigación sobre fraudes, delitos informáticos y vulnerabilidades que se presentan actualmente en las organizaciones públicas, privadas y mixtas, proponer políticas públicas que permitan tomar acciones preventivas y contribuir al desarrollo de las actividades empresariales, dado al elevado crecimiento de ataques cibernéticos en el mundo entero.

RECOMENDACIONES

- Se recomienda a la Universidad de las Fuerzas Armadas ESPE conjuntamente con los administradores y personal encargado de seguridad de TIC, fomentar la vinculación a través de campañas o talleres de concientización en materia de seguridad informática, creando una cultura tecnológica empresarial, previniendo posibles intromisiones y la detección de intrusos.

- A los administradores, contratar cualquier tipo de mecanismo en seguridad de los sistemas de protección de información, como son firewalls o cortafuegos de manera continua, ya que ayudarán a mantener a los ciberdelincuentes alejados de la información, prevenir ataques externos en las redes locales, todo esto dependiendo del volumen de operaciones y su actividad industrial.

- Se recomienda la adopción de la guía de buenas de prácticas en Tecnología de Información y Comunicación propuesta por los investigadores del proyecto, ya que al hacer uso de este instrumento ayudará en gran medida y de manera íntegra a la gestión de tecnologías, implementación de herramientas de seguridad informática, mitigación de riesgos cibernéticos y fraudes informáticos.

Gracias

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA