UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORAS:

TANIA STEFANÍA COFRE SANTO

VICTORIA CAROLINA REMACHE SOTO

DIRECTOR:

ECON. FRANCISCO CAICEDO A.

2018

"El sabio no dice todo lo que piensa, pero siempre piensa todo lo que dice"

Aristóteles

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

TEMA: "ANÁLISIS DEL COSTO-BENEFICIO DE LAS EMPRESAS DEL SECTOR SERVICIOS REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍAS QUE UTILIZAN HERRAMIENTAS DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA PROVINCIA DE COTOPAXI DURANTE EL PERIODO 2012-2016"

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

PLANTEAMIENTO DEL PROBLEMA

Macro Contextualización

Sistemas operativos desactualizados de empresas, especialmente en Rusia, Ucrania y Taiwán

Meso Contextualización

Colombia es el tercer país más afectado por ataque informáticos. La Seguridad informática no es una fortaleza, sino una debilidad.

Micro contextualización

En Ecuador se propagó un virus denominado 'malware' y en cinco días penetró en los ordenadores de unas 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca

FORMULACIÓN DEL PROBLEMA

¿Cómo incide la aplicación de herramientas de seguridad de la información en la rentabilidad de las empresas del sector servicios reguladas por la Superintendencia de Compañías y la SEPS?

JUSTIFICACIÓN

- Superintendencia de Compañías
- Superintendencia de Economía Popular y solidario

Inversión en herramientas de seguridad y protección de datos

Seguridad informática es un aspecto que está cada vez más expuesto a robos, modificación o eliminación de información.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

OBJETIVOS

OBJETIVO GENERAL

Analizar el costo – beneficio de invertir en herramientas de Seguridad y Protección de Datos en las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía, Popular y Solidaria, en la Provincia de Cotopaxi durante el periodo 2012-2016, para proponer un simulador que permita conocer el retorno de la inversión en Seguridad de la Información

OBJETIVOS

OBJETIVO ESPECIFICOS

- Definir las bases teóricas que permitan afianzar el estudio de la investigación sobre el Costo- Beneficio de herramientas de seguridad y protección de datos de las empresas del sector de servicios reguladas por la Superintendencia de Compañías.
- Identificar las características y porcentajes de inversión en seguridad informática de las empresas del sector servicios reguladas por la Superintendencia de Compañías y la SEPS para un correcto desarrollo del trabajo investigativo
- Determinar en base a la norma ISO (Organización Internacional de Normalización) 27002, los controles de seguridad de la información que utilizan las empresas del sector servicios reguladas por la Superintendencia de Compañías y la SEPS en la Provincia de Cotopaxi.

OBJETIVOS

OBJETIVO ESPECIFICOS

- Establecer el costo y el beneficio marginal de invertir en herramientas de seguridad y protección de datos que utilizan las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la SEPS en la Provincia de Cotopaxi.

- Proponer un simulador para conocer el retorno de la inversión de la seguridad de la información y protección de datos para proporcionar a las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la SEPS un instrumento de consulta al invertir en seguridad informática.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CAPÍTULO II

MARCO TEÓRICO

FUNDAMENTACIÓN CONCEPTUAL

Datos / información

Herramientas de seguridad

Inversión

ROSI

(Retorno de Inversión en Seguridad)

Controles de ISO/IEC 27002

Base Legal

- Art 66 numeral 3, 19, 20.

Constitución de la República del Ecuador

- Objetivo N°6

Plan Nacional del Buen Vivir

- En proyecto

Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales

VARIABLES DE LA INVESTIGACIÓN

V. DEPENDIENTE

Costo-Beneficio

V. INDEPENDIENTE

Inversión en la aplicación de herramientas de seguridad y protección de datos

HIPÓTESIS

Hipótesis alternativa (H_1)

La inversión en herramientas de seguridad y protección de datos genera un costo-beneficio marginal a las empresas del sector servicios reguladas por la Superintendencia de Compañías y por la SEPS de la provincia de Cotopaxi.

Hipótesis nula (H_0)

La inversión en herramientas de seguridad y protección de datos no genera un costo-beneficio marginal a las empresas del sector servicios reguladas por la Superintendencia de Compañías y por la SEPS de la provincia de Cotopaxi.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

METODOLOGÍA

- **ENFOQUE**
  - Cuantitativo
  - Cualitativo
- **MODALIDAD**
  - *Bibliográfica-documental
  - *De Campo
- **TIPO DE INVESTIGACIÓN**
  - *Exploratoria
  - *Descriptiva
- **TÉCNICA DE INVESTIGACIÓN**
  - Cuestionario

POBLACIÓN

Empresas de Servicios: Reguladas por la Superintendencia de Compañías
Reguladas por la SEPS (Segmentos uno, dos, tres y cuatro)

MUESTRA

Muestreo Intencional

Entidades reguladas por la Superintendencia de Compañías

RAMO / ACTIVIDAD	DENOMINACIÓN	EMPRESA
Actividades de servicio administrativos y de apoyo	Caso de estudio 23	Seilatacunga Cia. Ltda.
Enseñanza	Caso de estudio 24	Eduquer-CERIT
Actividades de atención de la salud humana y de asistencia social	Caso de estudio 25	Centro de Diálisis Contigo CENDIALCON Cia. Ltda.
Actividades de alojamiento y de servicio de comidas	Caso de estudio 26	Hostería La Ciénega

Fuente: (Superintendencia de Compañías, 2016)

Entidades reguladas por la SEPS.

SEGEMENTO	DENOMINACIÓN	COOPERATIVA DE AHORRO Y CRÉDITO
Segmento 1	Caso de estudio 1	De la Pequeña Empresa de Cotopaxi Ltda.
Segmento 2	Caso de estudio 2 Caso de estudio 3	Virgen del Cisne 9 de Octubre
Segmento 3	Caso de estudio 4 Caso de estudio 5 Caso de estudio 6 Caso de estudio 7 Caso de estudio 8	Educadores Primarios del Cotopaxi Sumak Kawsay Ltda. Andina Ltda. Sierra Centro Ltda. Visión de los andes Visandes
Segmento 4	Caso de estudio 9 Caso de estudio 10 Caso de estudio 11 Caso de estudio 12 Caso de estudio 13 Caso de estudio 14 Caso de estudio 15 Caso de estudio 16 Caso de estudio 17 Caso de estudio 18 Caso de estudio 19 Caso de estudio 20 Caso de estudio 21 Caso de estudio 22	Unión Mercedaria Ltda. Pilahuin 15 de Agosto de Pilacoto Pujili Ltda. Iliniza Ltda. Uniblock y servicios Ltda. Coorcotopaxi Ltda. Pucara Ltda. Sinchi runa Ltda. Santa Rosa de Patutan Ltda. Integración Solidaria Ltda. Indígena Sac Latacunga Ltda. Credil Ltda. Monseñor Leónidas Proaño

Fuente: (Superintendencia de Economía Popular y Solidaria, 2016)

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CAPÍTULO IV

RESULTADOS

COMPROBACIÓN DE HIPÓTESIS

PROCEDIMIENTO CON SPSS

			29) Actualmente se aplica herramientas de S.I en la entidad		Total
			No	Si	
8) ¿Cuánto es el monto de inversión, que fue asignado para la seguridad de la información, durante el periodo 2012 al 2016?	Menos de $5.000	Recuento	1	10	11
		Recuento esperado	,8	10,2	11,0
	De $5.000 a $ 15.000	Recuento	0	7	7
		Recuento esperado	,5	6,5	7,0
	De $15.000 a $30.000	Recuento	0	4	4
		Recuento esperado	,3	3,7	4,0
	De $30.000 a $40.000	Recuento	0	2	2
		Recuento esperado	,2	1,8	2,0
	Mayores a $40.000	Recuento	0	1	1
		Recuento esperado	,1	,9	1,0
	No aplica	Recuento	1	0	1
		Recuento esperado	,1	,9	1,0
Total		Recuento	2	24	26
		Recuento esperado	2,0	24,0	26,0

COMPROBACIÓN DE HIPÓTESIS

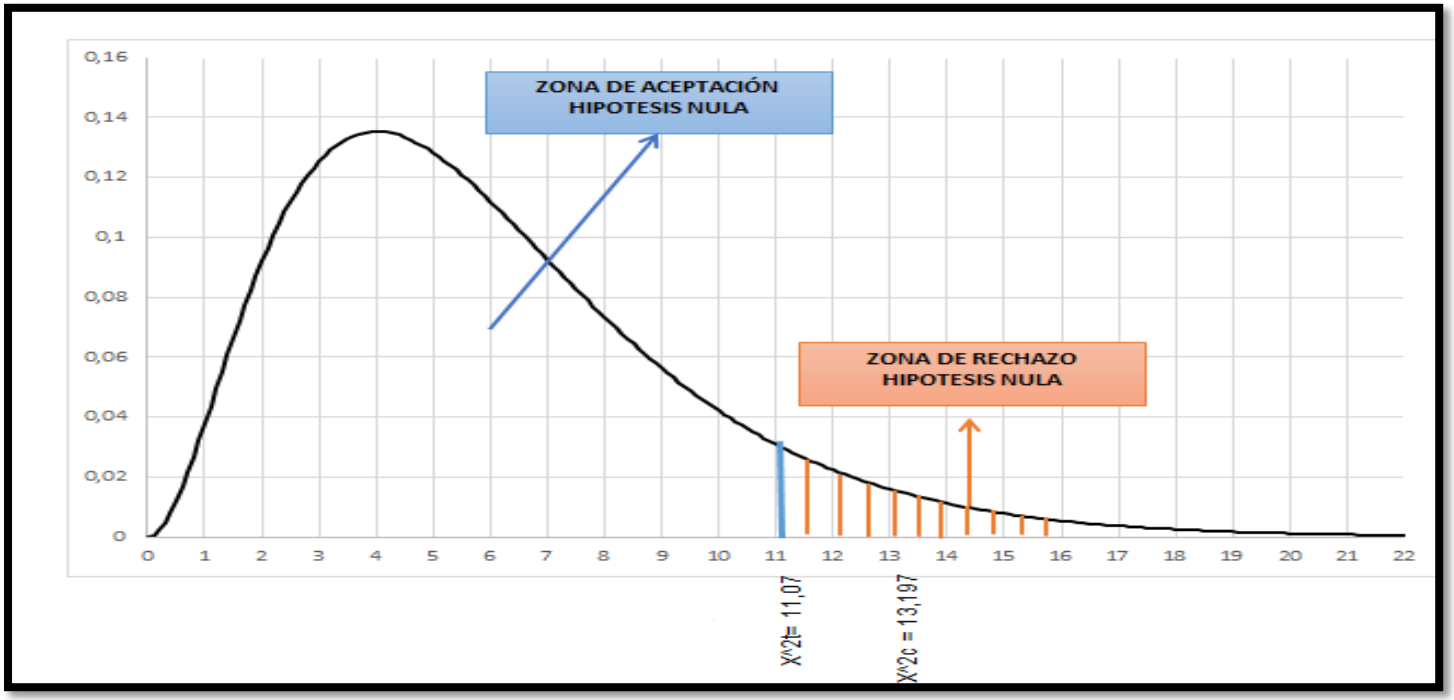
	Valor	gl.	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	13,197[a]	5	,022
Razón de verosimilitud	7,400	5	,193
Asociación lineal por lineal	2,071	1	,150
N° de casos válidos	26		

a. 10 casillas (83,3%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,08.

CHI - CRÍTTICO

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
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916

COMPROBACIÓN DE HIPÓTESIS



X2c=13,197 **>** X2t= 11,07

Decisión: Se rechaza la Hipótesis Nula (Ho) y se acepta la Hipótesis Alternativa (H1), que dice: La inversión en herramientas de seguridad y protección de datos si genera un beneficio marginal a las empresas del sector servicios reguladas por la Superintendencia de Compañías y por la SEPS de la provincia de Cotopaxi.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CAPÍTULO V

PROPUESTA

Diseño de una matriz costo- beneficio, en base a los incidentes y controles de la ISO 27002 no aplicados en los casos de estudio, y la creación de un simulador de inversión para Seguridad de la Información, orientados a establecer un presupuesto estimado de inversión en soluciones para mitigar en cierta medida los riesgos más comunes a los que están expuestos las entidades.

Modelo Operativo de la Propuesta

FASES	OBJETIVOS	DESCRIPCIÓN DE ACTIVIDADES
FASE I	Determinar los controles de la Norma ISO 27002 no aplicados y los incidentes de seguridad producidos, formulando políticas, lineamientos y demás medidas para hacer frente a los problemas de seguridad de la información.	Detallar las principales debilidades detectadas por grupo de empresas luego de aplicar los distintos métodos de análisis y recolección de información. Formular políticas y lineamientos de seguridad que son una parte importante para el éxito de la operatividad en las empresas.
FASE II	Elaborar una matriz costo-beneficio para evaluar el impacto económico de adquirir una herramienta para proteger los activos de la información.	En función de los incidentes mayormente ocurridos por grupo de empresas, se detalla el costo promedio del incidente estos datos son obtenidos directamente de las encuestas, Se enuncia los costos de inversión conseguidos a través de empresas proveedoras de herramientas de seguridad con estos datos Se determina el beneficio marginal luego de aplicar el cálculo del indicador ROSI.
FASE III	Desarrollar un simulador de inversión en Microsoft Excel que posibilite el cálculo de los costos y el beneficio marginal en seguridad de la información	Instrucciones para usar correctamente el simulador. Plantilla de datos. Usar fórmulas y funciones del Excel. Ejecución del simulador de inversión.

Problemas de seguridad para proteger la información

Fase I Determinar los controles de la Norma ISO 27002 no aplicados y los incidentes de seguridad producidos.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

SEGMENTO 1

ACTIVOS MAYORES A $80´000.000 → 6

SEGMENTO 2

ACTIVOS MAYORES A 20'000.000,00 hasta 80'000.000,00 → 5

SEGMENTO 3

ACTIVOS MAYORES a 1'000.000,00 hasta 5'000.000,00 → 11

SEGMENTO 4

ACTIVOS MAYORES A 1'000.000,00 HASTA 5'000.000,00 → 14

SUPERINTENDENCIA DE COMPAÑÍAS

11

- Actividades administrativas y de Apoyo
- Enseñanza
- Salud
- Alojamiento

Políticas y Lineamientos

PROBLEMAS	POLÍTICAS	LINEAMIENTOS
Ausencia de políticas de uso de controles criptográficos	Asegurar la integridad y la confidencialidad de la información que maneja la entidad	Para lograr la integridad y la confidencialidad se aplicarán mecanismos de criptografía, en el uso de páginas web se aplicarán certificados digitales, en las conexiones de red inalámbrica se aplicarán controles de cifrado que no hayan sido detectados como vulnerables.
No tienen un método o programa para borrar la información.	Eliminación o destrucción segura de la información confidencial de la empresa.	Se usaran métodos o programas de borrado de información sensible que certifiquen la eliminación permanente de los datos, previo a un seguimiento de los activos de datos que han llegado al final de su ciclo de vida y luego destruirlos en su origen de manera que esta información no sea recuperable.
Administración y control de red/Ingreso al sistema de otras áreas.	Toda empresa debe segmentar y asegurar las conexiones de redes tanto internas como externas y así evitar fugas de información que pueden afectar social o económicamente a una empresa.	Para segmentar la red se debe limitar las áreas comprendidas, dependiendo del tipo de información que maneja, y para asegurar las conexiones inalámbricas establecer mecanismos de identificación y autenticación, como la asignación de un ID de usuario propio, y contraseñas que no hayan sido reutilizadas, y que al mismo tiempo son confidenciales.

PROBLEMAS	POLÍTICAS	LINEAMIENTOS
Los ordenadores se actualizan automáticamente	Las nuevas implementaciones o actualizaciones de software debe estar sujetas a revisión.	Toda actualización del sistema operativo debe ser revisada su compatibilidad con los programas que utiliza la empresa para su posterior instalación en los equipos.
Comunica eventos de inseguridad a todo el personal.	Todo comunicado que se efectué en la entidad debe ser transmitido únicamente al personal correspondiente	Al presentarse un fallo o incidente de seguridad de la información se debe realizar un reporte el cual debe entregarse personalmente al Depto. de Seguridad Informática o únicamente al personal encargado en solucionar el problema.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Herramientas de seguridad y Protección de Datos

SOLUCIÓN	COSTOS
Políticas de uso de controles criptográficos	
Criptografía para página Web	$ 130,00
Configuración Red inalámbrica y red local	$ 200,00
Concienciación, educación y capacitación en S.I	
Charla sobre ingeniería social, fraude o phishing	$ 200,00
Charla sobre el uso indebido de la información crítica	$ 200,00
Capacitación en procedimientos de seguridad de la información.	$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 máquinas	$ 40,00
Inventario de Activos	
Base de datos para control de inventario	$ 1.200,00
Eliminación de Soportes	
Método o programa para el borrado de información confidencial	$ 24,00
Protección de los registros de información	
Equipo servidor	$ 2.000,00
Configuraciones	$ 1.500,00
Segregación de redes	
Router	$ 500,00
Switch	$ 200,00
Rack	$ 400,00
Patch Panel	$ 80,00
Configuraciones	$1.000,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina	$ 70,00
Licencia Paquete Office por máquina	$ 90,00
Copias de seguridad de la información	
Sistemas backup (Dvds, usb, Alojamiento en línea)	$ 200,00
Gestión de contraseñas de usuario	
Gestor de contraseñas manual	$ 20,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	$ 100,00
Controles de acceso	
Equipo servidor	$ 2000,00
Configuraciones (ACL-Proxy)	$ 800,00
Controles físicos de entrada	
Lector biométrico	$ 400,00

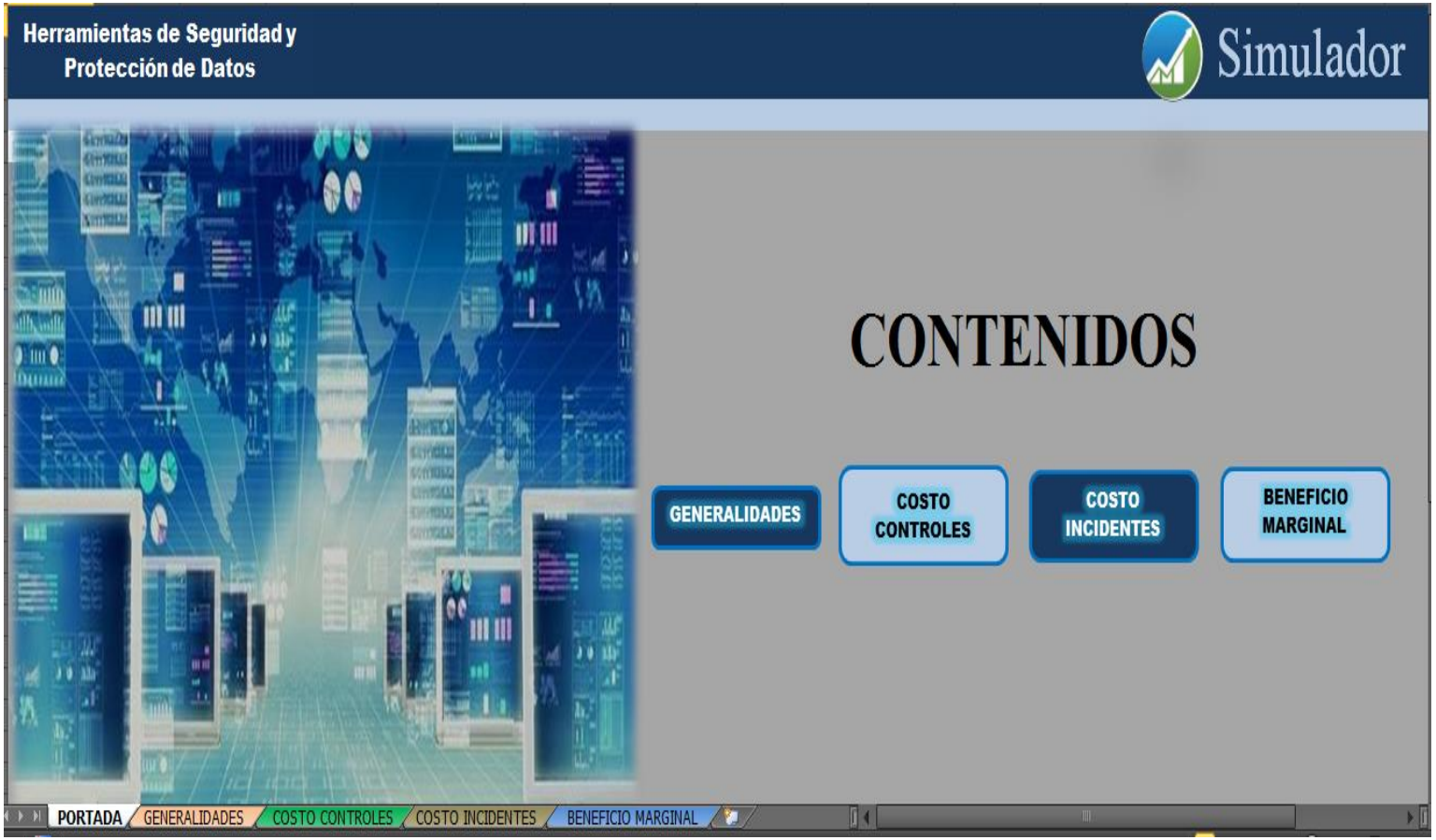
Datos actualizados a Marzo del 2018 por el Ing. Cristian Gallado

Fase II Elaborar una matriz costo-beneficio

ORGANISMO REGULADOR	EMPRESAS	Número de problemas	COSTO PROBLEMAS EN S.I (2012-2016)	COSTO INVERSIÓN	BENEFICIO MARGINAL (ROSI)
Superintendencia de Economía Popular y Solidaria	Segmento 1	6	$20.000	$9.030	84,56%
	Segmento 2	5	$15.000	$5.730	109,42%
	Segmento 3	11	$12.000	$5.350	103,81%
	Segmento 4	14	$9.000	$3.854	116,85%
Superintendencia de Compañías	Salud, Enseñanza, Alojamiento y actividades administrativas	11	$15.000	$6.660	104,75%

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Fase III Desarrollar un simulador de inversión



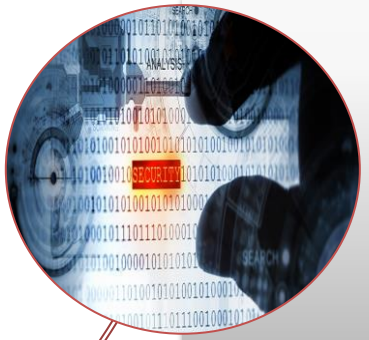
CONCLUSIONES

Al iniciar el estudio de inversión en Herramientas de Seguridad y protección de Datos con el análisis del balance general de cada empresa de servicios se identificó, que no se desglosa las cuentas ni los montos relacionados con el software, licencias y demás elementos que dan seguridad a la información, por tal motivo para la investigación se tomó como referencia la cuenta equipo de cómputo.

Dos cooperativas de ahorro y crédito del segmento cuatro no aplican ninguna herramienta o mecanismo de seguridad y protección de datos, del resto de entidades 21 empresas utilizan el antivirus como medida de seguridad de la información, sin embargo entre el periodo 2012 - 2016 se obtuvo como resultado de la encuesta, 15 casos de ataque o infección por código malicioso por año, siendo evidente que la herramienta utilizada no ayuda a combatir el incidente.

CONCLUSIONES

De los controles menos implementados de la norma ISO 27002 en las empresas de servicios, el 61,54% no utiliza criptografía para el cifrado de datos, el 57,69% no cuenta con un método o programa para borrar la información confidencial, el 53,85% no tienen segmentada la red de la empresa, el 61,54% no utilizan un gestor de contraseñas, el 61,54% los ordenadores se actualizan automáticamente y el 80,77% comunica los eventos de inseguridad a todo el personal provocando conmoción.



De acuerdo al estudio se concluye que en el segmento uno, las entidades presentan 6 problemas relacionados a la seguridad de la información y en el segmento dos existen 5 problemas, por otro lado el segmento tres presenta 11 problemas de seguridad, el segmento cuatro tiene 14 y las entidades reguladas por la Superintendencia de Compañías tienen 11 inconvenientes en seguridad de la información.

RECOMENDACIONES

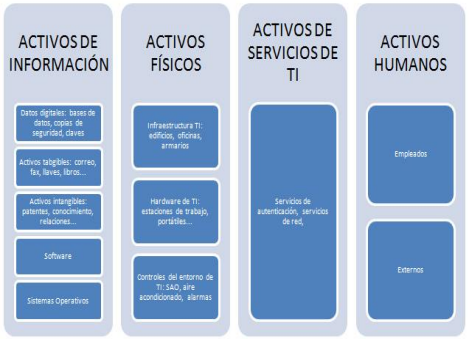
Las empresas para su registro contable, deben reestructurar su plan de cuentas, creando subcuentas específicas que detallen los montos correspondientes del software, licencias y demás herramientas de seguridad y protección de datos, para tener un mejor control financiero de los activos intangibles con las que cuenta la organización.

Las herramientas de seguridad y protección de datos no requieren únicamente ser implementadas, sino más bien deberán ser evaluados y monitoreados de manera continua, buscando acciones de cambio correctivas orientadas a la optimización de las herramientas utilizadas.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

RECOMENDACIONES

En las empresas indistintamente al sector económico al que pertenecen, cada departamento debe clasificar y elaborar un inventario de activos de información, que permitan el control y administración efectiva, garantizando la disponibilidad, integridad, y confidencialidad de los datos, esto es necesario porque en función de su criticidad se aplicará diferentes herramientas o medidas de seguridad para proteger la información, los controles deberán ser evaluados y monitoreados de manera continua.



Los organismos reguladores deben promover un cambio de cultura en el nivel gerencial, especialmente en las empresas del segmento tres, cuatro y las entidades dedicadas a actividades de alojamiento, administrativas, educación y salud, mediante la aplicación de programas de capacitación que den a conocer, la importancia y los riesgos de no proteger la información crítica y sensible de las entidades.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA