



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

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

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

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

**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”**

AUTORAS:

**TANIA STEFANÍA COFRE SANTO
VICTORIA CAROLINA REMACHE SOTO**

DIRECTOR: ECON. FRANCISCO CAICEDO

LATACUNGA

2018



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

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

CERTIFICADO

Certifico que el trabajo de titulación, **“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”** realizado por la señorita **TANIA STEFANÍA COFRE SANTO** y por la señorita **VICTORIA CAROLINA REMACHE SOTO**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas – ESPE, por lo tanto me permito acreditarlo y autorizar a la señorita **TANIA STEFANÍA COFRE SANTO** y a la señorita **VICTORIA CAROLINA REMACHE SOTO** para que lo sustenten públicamente.

Latacunga, Mayo del 2018

Atentamente,


Econ. Francisco Caicedo A.
DIRECTOR



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

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

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORÍA DE RESPONSABILIDAD

Nosotros, **TANIA STEFANÍA COFRE SANTO**, con cédula de ciudadanía N° 055000683-7 y **VICTORIA CAROLINA REMACHE SOTO**, con cédula de ciudadanía N° 055000806-4, declaramos que este trabajo de titulación **“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”**, ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Latacunga, Mayo del 2018

Tania Stefania Cofre Santo

C.C.: 055000683-7

Victoria Carolina Remache Soto

C.C.: 055000806-4



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

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORIZACIÓN

Nosotros, **TANIA STEFANÍA COFRE SANTO** y **VICTORIA CAROLINA REMACHE SOTO**, autorizamos a la Universidad de las Fuerzas Armadas – ESPE publicar en la biblioteca virtual de la institución el presente trabajo de titulación “**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**”, cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Latacunga, Mayo del 2018

Tania Stefania Cofre Santo

C.C.: 055000683-7

Victoria Carolina Remache Soto

C.C.: 055000806-4

DEDICATORIA

Con infinito amor dedico este trabajo de titulación a Dios quien me ha dado salud, sabiduría y ha derramado en mí muchas bendiciones para culminar esta meta con éxito, también por darme unos padres maravillosos Juan Cofre y Lucrecia Santo, quienes con su ejemplo de trabajo, humildad, y sacrificio me han sabido formar como un gran ser humano, inculcando en mí valores, dedicando su vida incondicionalmente para darme lo mejor, enseñándome el valor de las cosas que tengo a mi alrededor y el trabajo que cuesta conseguirlas, que nada surge de la nada, todo es a base del esfuerzo del día a día, por todo esto y más mi enorme gratitud con mis queridos padres a quienes amo y respeto mucho. A mis hermanos Daniela, Fernando y Eduardo quienes han sido mi motivación para hacer las cosas bien y convertirme así en su modelo de superación, a mis maestros quienes nos han sabido impartir sus conocimientos profesionales y de vida, finalmente a mis amigas por ser una parte fundamental en mi existencia, llenar mis días de felicidad y su compañía incondicional en este continuo proceso de aprendizaje.

Tania

DEDICATORIA

El trabajo de titulación se la dedico a Dios por cada nuevo amanecer que me ha regalado, es un fiel amigo que me acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de dificultad y por las bendiciones recibidas.

Este logro alcanzado se los debo a mis padres Edgar Remache y Germania Soto porque creyeron en mí y sacrificaron sus vidas para permitir que yo pudiera tener un mejor futuro, los amo mucho y nunca dejaré de estar agradecida por su apoyo incondicional tanto moral y económicamente, mis padres son mis primeros maestros que me formaron con valores para ser cada día mejor y me enseñaron que el camino es difícil pero de mi depende que con esfuerzo y dedicación es posible levantarse y continuar caminando por el sendero de la vida.

A mi hermana porque me ha extendido su mano y no me ha dejado sola en los momentos de dificultad, por ser mi gran amiga, confidente y ejemplo a seguir.

A mis abuelitos por sus consejos, generosidad, apoyo, y por haberme enseñando la esencia de la vida, tienen un valor incalculable, que me ha permitido ser cada día mejor persona y ver hoy alcanzada una de mis metas.

A mis demás familiares tíos, primos y amigos que desean lo mejor en cada paso que doy, constantemente me están motivando para seguir superándome y hacer realidad mis sueños.

Carolina

AGRADECIMIENTO

Expresamos nuestro más profundo y sincero agradecimiento a la Universidad de las Fuerzas Armadas ESPE-Latacunga por abrirnos las puertas y formarnos como profesionales de excelencia.

Al proyecto de investigación “Tecnología de Información y Comunicación, impacto en la economía de las empresas de la provincia de Cotopaxi”, aprobado por el Consejo de Departamento de Ciencias Económicas Administrativas y de Comercio, según resolución N° 003-2017-ESPE-DECEAC del 28 de marzo del 2017, el trabajo de titulación orienta a las empresas de servicios en mejorar la gestión de herramientas de seguridad y protección de datos, para lo cual se ha diseñado un simulador de inversión, generando resultados inmediatos sobre el costo – beneficio.

A nuestro tutor Eco. Francisco Caicedo, por sus enseñanzas, paciencia y motivación brindada, que han sido esenciales para la culminación del trabajo de titulación.

Al Ing. Cristian Gallardo docente del grupo de investigación ARSI (Automatización, Robótica y Sistemas Inteligentes) de la Universidad de las Fuerzas Armadas ESPE-Latacunga, por sus conocimientos impartidos y orientación en cada etapa del desarrollo de la investigación.

Al Ing. Luis Lema Director del Macro-proyecto por su tiempo y dedicación brindada, por darnos la oportunidad de formar parte de su trabajo de investigación y aprender sobre temas de tecnología que van a la vanguardia frente al incremento y las nuevas formas de ataques cibernéticos.

A todos nuestros profesores que nos enseñaron tanto de la profesión así como también de la vida.

A las diferentes instituciones que nos dieron la apertura y proporcionaron la información necesaria para cumplir los objetivos del trabajo de titulación.

Estamos eternamente agradecidas con Dios, nuestros padres, familiares y amigos que siempre nos brindaron su apoyo incondicional, y hoy podemos ver culminada nuestra meta de tener el título profesional.

ÍNDICE DE CONTENIDOS

PORTADA	i
CERTIFICADO	ii
AUTORÍA DE RESPONSABILIDAD	iii
AUTORIZACIÓN	iv
DEDICATORIA	v
DEDICATORIA	vi
AGRADECIMIENTO	vii
ÍNDICE DE CONTENIDOS	viii
ÍNDICE DE TABLAS	xii
ÍNDICE DE FIGURAS	xiv
RESUMEN	xvi
ABSTRACT	xvii

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN	1
1.1. Tema de investigación	1
1.2. Antecedentes	1
1.3. Planteamiento del problema.....	5
1.3.1. Macro Contextualización	5
1.3.2. Meso Contextualización	7
1.3.3. Micro contextualización	9
1.3.4. Árbol de problemas	11
1.4. Formulación del problema.....	11
1.5. Justificación.....	11
1.6. Delimitación de la investigación	12
1.7. Objetivos	13
1.7.1. Objetivo general	13
1.7.2. Objetivos específicos	13

CAPÍTULO II

2. MARCO TEÓRICO	14
2.1. Fundamentación Teórica.....	14
2.1.1. Normas ISO/IEC 27000.....	14
2.1.2. ISO/IEC 27001	14

2.1.3.	ISO/IEC 27002	14
2.1.4.	Controles de ISO/IEC 27002	15
a.	Políticas de Seguridad	15
b.	Aspectos organizativos de la Seguridad de la Información	15
c.	Seguridad ligada a los recursos humanos	16
d.	Gestión de activos	17
e.	Control de Accesos	19
f.	Cifrado.....	20
g.	Seguridad física y ambiental.	20
h.	Seguridad en la operativa	22
i.	Seguridad en las Telecomunicaciones.....	25
j.	Adquisición, desarrollo y Mantenimiento de los sistemas de información.....	26
k.	Relaciones con Suministradores.....	28
l.	Gestión de Incidentes.....	29
m.	Aspectos de la SI en la Gestión de la Continuidad de Negocio	30
n.	Cumplimiento	31
2.1.5.	ISO/IEC 27003	32
2.1.6.	ISO/IEC 27004	32
2.1.7.	ISO/IEC 27005	32
2.1.8.	ISO/IEC 27006	33
2.2.	Marco conceptual	33
2.2.1.	Seguridad informática	33
2.2.2.	Objetivos de la seguridad de la información.....	34
2.2.3.	Importancia de la seguridad de la información.....	36
2.2.4.	Entidades implicadas en la seguridad y protección de la informac .	36
2.2.5.	Datos.....	37
2.2.6.	Información	37
a.	Clasificación de la Información.....	37
2.2.7.	Herramientas de seguridad	38
a.	Mecanismos de Seguridad lógica	39
b.	Mecanismo de Seguridad Física	40
2.2.8.	Análisis y gestión de riesgos en un sistema informático	41
a.	Amenazas	41
b.	Vulnerabilidades.....	42
c.	Incidentes de seguridad	43
d.	Impactos.....	43

e.	Defensas, salvaguardias o medidas de seguridad.....	43
2.2.9.	Presupuesto- Inversión en Seguridad de la Información.....	43
a.	Inversión.....	43
b.	Presupuesto de inversiones.....	44
2.2.10.	Beneficio - Retorno de Inversión en Seguridad (ROSI).....	45
2.2.11.	Organismos de Control.....	45
a.	Superintendencia de Compañías.....	45
b.	Superintendencia de Economía Popular y Solidaria (SEPS).....	46
2.3.	Base Legal.....	47
2.3.1.	Constitución de la República del Ecuador.....	47
2.3.2.	Plan Nacional del Buen Vivir.....	48
2.3.3.	Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales.....	48
2.3.4.	Ley Orgánica de Transparencia y Acceso a la Información P.....	48
2.3.5.	Ley del Sistema Nacional de Registros de Datos Públicos.....	48
2.3.6.	Ley Orgánica de la Gestión de la Identidad y Datos Civiles.....	49
2.3.7.	Código Orgánico Integral Penal.....	49
2.4.	Sistemas de variables.....	49
2.4.1.	Variable dependiente.....	49
2.4.2.	Variable independiente.....	49
2.5.	Hipótesis.....	50
2.5.1.	Hipótesis alternativa (H_1).....	50
2.5.2.	Hipótesis nula (H_0).....	50
2.6.	Operacionalización de variables.....	50

CAPÍTULO III

3.	METODOLOGÍA DE LA INVESTIGACIÓN.....	52
3.1.	Enfoque de la investigación.....	52
3.2.	Modalidad de la investigación.....	52
3.2.1.	Bibliográfica – documental.....	52
3.2.2.	De campo.....	53
3.3.	Nivel o tipo de investigación.....	53
3.3.1.	Investigación exploratoria.....	53
3.3.2.	Investigación descriptiva.....	54
3.4.	Población y Muestra.....	54
3.4.1.	Población.....	54
3.4.2.	Muestra.....	55

3.1.	Fuentes de información	57
3.5.	Técnicas de recopilación de información	57
3.5.1.	Instrumentos de la investigación	57
3.5.2.	Definición de los sujetos/unidades de información.....	58
3.5.3.	Validación y confiabilidad.....	58
3.6.	Técnicas de análisis de datos	59
3.7.	Técnicas de comprobación de hipótesis	59

CAPÍTULO IV

4.	RESULTADOS DE LA INVESTIGACIÓN.....	60
4.1.	Análisis de la estructura organizativa de las empresas.....	60
4.2.	Análisis del crecimiento en equipo de cómputo	69
4.3.	Análisis de los resultados de la encuesta	75
4.4.	Comprobación Hipótesis	119

CAPÍTULO V

5.	PROPUESTA.....	123
5.1.	Datos informativos.....	123
5.2.	Antecedentes de la propuesta.....	124
5.3.	Justificación.....	124
5.4.	Objetivos de la propuesta.....	125
5.4.1.	Objetivo General	125
5.4.2.	Objetivos Específicos	125
5.5.	Diseño de la propuesta	126
5.5.1.	FASE I: Determinar los controles de la Norma ISO 27002 no aplicados y los incidentes de seguridad producidos.	127
5.5.2.	FASE II Elaborar una matriz costo-beneficio.....	153
5.5.3.	FASE III Desarrollar un simulador de inversión	154

CAPÍTULO VI

6.	CONCLUSIONES Y RECOMENDACIONES.....	161
6.1	Conclusiones.....	161
6.2.	Recomendaciones	163

SIGLAS Y ABREVIATURAS.....	166
-----------------------------------	------------

REFERENCIAS BIBLIOGRÁFICAS	167
---	------------

ANEXOS.....	172
--------------------	------------

ÍNDICE DE TABLAS

Tabla 1 Segmentación de entidades del SFPS	47
Tabla 2 Cuadro de Operacionalización de variables.....	50
Tabla 3 Entidades reguladas por la SEPS.....	56
Tabla 4 Entidades reguladas por la Superintendencia de Compañías	56
Tabla 5 Estructura organizacional entidades de alojamiento	62
Tabla 6 Entidades organizacional entidades de enseñanza	64
Tabla 7 Estructura organizacional entidades de salud.....	65
Tabla 8 Estructura organizacional entidades de Administración	66
Tabla 9 Estructura organizacional Cooperativas de Ahorro y Crédito.....	67
Tabla 10 Crecimiento equipo de cómputo – Segmento 1	69
Tabla 11 Crecimiento equipo de cómputo – Segmento 2	70
Tabla 12 Crecimiento equipo de cómputo – Segmento 3	71
Tabla 13 Crecimiento equipo de cómputo – Segmento 4	72
Tabla 14 Crecimiento equipo de cómputo – Entidades de la CIA	74
Tabla 15 Aplicación de Políticas de Seguridad de la Información	76
Tabla 16 Departamento encargado de la S.I	79
Tabla 17 Accesos dados de baja	81
Tabla 18 Herramientas de S.I	82
Tabla 19 Herramientas de S.I	83
Tabla 20 Inversión en Seguridad de la Información.....	86
Tabla 21 Incidentes y Brechas de Seguridad de la Información	89
Tabla 22 Costos Incidentes de S.I	91
Tabla 23 Presupuesto anual S.I.....	93
Tabla 24 Términos y condiciones Contrato Laboral.....	94
Tabla 25 Términos y condiciones acuerdo confidencialidad.....	95
Tabla 26 Tipo de información.....	96
Tabla 27 Controles criptográficos	98
Tabla 28 Activos de la Información	99
Tabla 29 Método_ programa borrado información	100
Tabla 30 Registro de intento de accesos.....	101
Tabla 31 Segmentación de red	103
Tabla 32 Soporte técnico externo – confidencialidad.....	104
Tabla 33 Protección cable eléctrico y telecomunicaciones	105
Tabla 34 Licencias originales.....	106
Tabla 35 Revisión de sistemas a ser implantados	107
Tabla 36 Copias de Seguridad.....	108
Tabla 37 Frecuencia copias de seguridad	109
Tabla 38 Gestor de contraseñas.....	110
Tabla 39 Actualización automática ordenadores	111
Tabla 40 Restricciones uso de internet.....	112
Tabla 41 Áreas seguras.....	113
Tabla 42 Comunicación eventos de inseguridad en la S.I	114

Tabla 43 Instalación Software.....	115
Tabla 44 Capacitación en S.I.....	116
Tabla 45 Proveedores de Herramientas de S.I.....	117
Tabla 46 Cruce de Variables.....	120
Tabla 47 Pruebas del Chi Cuadrado.....	121
Tabla 48 Modelo Operativo de la Propuesta.....	127
Tabla 49 Matriz Costo – Beneficio	153

ÍNDICE DE FIGURAS

Figura 1. Árbol de problemas.....	11
Figura 2. Fórmula para el cálculo del ROSI	45
Figura 3. Crecimiento equipo de cómputo – Segmento 1	69
Figura 4. Crecimiento equipo de cómputo – Segmento 2	70
Figura 5 Crecimiento equipo de cómputo – Segmento 3	71
Figura 6. Crecimiento equipo de cómputo – Segmento 4	73
Figura 7. Crecimiento equipo de cómputo– Entidades de la SC.....	74
Figura 8. Aplicación de políticas de Seguridad de la Información.....	77
Figura 9. Departamento encargado de la S.I	80
Figura 10. Accesos dados de baja.....	81
Figura 11. Aplicación de Herramientas de S.I.....	82
Figura 12. Herramientas de S.I.....	85
Figura 13. Inversión en Seguridad de la Información.....	87
Figura 14. Incidentes y Brechas de Seguridad de la Información	90
Figura 15. Costos incidentes de S.I	92
Figura 16. Presupuesto anual de S.I.....	93
Figura 17. Términos y condiciones Contrato Laboral.....	94
Figura 18. Términos y condiciones acuerdo confidencialidad.....	95
Figura 19. Tipo de información	97
Figura 20. Controles criptográficos	98
Figura 21. Activos de la información	99
Figura 22. Método _ programa borrado información.....	100
Figura 23. Registro e intentos de accesos.....	102
Figura 24. Segmentación de red.....	103
Figura 25. Soporte técnico externo - confidencialidad	104
Figura 26. Protección cables eléctricos y telecomunicaciones	105
Figura 27. Licencias originales.....	106
Figura 28. Revisión de sistemas a ser implantados.....	107
Figura 29. Copias de Seguridad	108
Figura 30. Frecuencia de copias de seguridad	109
Figura 31. Gestor de contraseñas.....	110
Figura 32. Actualización automática ordenadores	111
Figura 33. Restricción uso de internet	112
Figura 34. Áreas seguras.....	113
Figura 35. Comunicación eventos de inseguridad en la S.I.....	114
Figura 36. Instalación Software.....	115
Figura 37. Capacitación en S.I	116
Figura 38. Proveedores de Herramientas de S.I.....	118
Figura 39. Regla de Decisión.....	121
Figura 40. Simulador- Hoja de contenidos.....	154
Figura 41 .Simulador – Hoja de Generalidades	154
Figura 42. Hoja controles ISO 27002 - Herramientas	157

Figura 43. Simulador Hoja de incidentes	157
Figura 44. Hoja incidentes – Matriz Costo	158
Figura 45. Hoja Beneficio –Matriz Beneficio	159

RESUMEN

En la actualidad la información es un recurso vital para toda empresa, este activo está situado en medios magnéticos y documentos que abarcan datos que pertenecen a la propia entidad, así como también de los trabajadores y clientes, siendo útiles para la operatividad de la empresa por lo tanto, se debe garantizar la confidencialidad, integridad y la disponibilidad de la información, a través de medidas de seguridad y herramientas necesarias para mitigar los riesgos evitando daños en la información. En tal sentido, el presente trabajo de titulación tiene como objetivo 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 SEPS, en la Provincia de Cotopaxi. A través de la información obtenida mediante la encuesta aplicada a 26 empresas de servicios, se pudo concluir que la inversión en herramientas de seguridad y protección de datos si genera un beneficio marginal. Además se identificó cada uno de los incidentes de seguridad más comunes, producidos anualmente en los últimos cuatro años y a partir de ello se estableció soluciones indicando los costos respectivos, y el presupuesto anual estimado de inversión. Finalmente se obtuvo el beneficio marginal a través del indicador ROSI (Retorno sobre la Inversión de Seguridad), para lo cual se trabajó por cada uno de los segmentos estudiados en cuanto a las Cooperativas de Ahorro y Crédito, así mismo para el grupo de entidades reguladas por la Superintendencia de Compañías.

PALABRAS CLAVE

- **EMPRESAS - INFORMACIÓN - SEGURIDAD**
- **RETORNO DE LA INVERSIÓN**
- **COOPERATIVAS DE AHORRO Y CRÉDITO**
- **EMPRESAS DE SERVICIOS**

ABSTRACT

Currently information is a vital resource for any company, this asset is located in magnetic media and documents that include data of the entity, workers and clients, being useful for the operation of the company, it must be ensure the confidentiality, integrity and availability of the information, through security measures and tools necessary to mitigate risks avoiding information damage, this degree work aims to analyze the cost / benefit of investment in security tools and data protection in the companies of the service sector regulated by the Superintendence of Companies and the SEPS, in the Province of Cotopaxi. From the information obtained through the survey applied to 26 service companies, it is concluded that the investment in security tools and data protection if it generates a marginal benefit. In addition, it identified the most common security incidents produced annually in the last four years then it was established solutions indicating the respective costs, and the estimated annual investment budget. Finally, the marginal benefit was obtained through the ROSI indicator (Return on the Security Investment), for which it worked with each of the segments of the Savings and Credit Cooperatives and the entities regulated by the Superintendence of Companies.

KEY WORDS

- **COMPANIES - INFORMATION - SECURITY**
- **RETURN ON INVESTMENT**
- **SAVINGS AND CREDIT COOPERATIVES**
- **SERVICE COMPANIES**

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1. Tema de investigación

“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”.

1.2. Antecedentes

Las herramientas de seguridad y protección de datos en las empresas indistintamente al sector económico al que pertenecen, evitan la pérdida o modificaciones no autorizadas de la información, caso contrario puede ocurrir eventos no deseados que pueden afectar tanto en lo económico así como también a la moral de aquellas personas que están involucradas con la organización, en este sentido las empresas necesitan un análisis del costo versus el beneficio de implementar herramientas de seguridad y protección de datos, permitiendo identificar la rentabilidad de la inversión y posteriormente de todas las opciones tomar la decisión de adquirir una nueva herramienta que represente un menor costo y un gran beneficio para la empresa.

El presente tema de investigación “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”, y adicionalmente considerando a las instituciones reguladas por la SEPS, se orienta en estudios de autores tanto nacionales así como también de nivel internacional, destacando una publicación del diario La Razón (2015) en esta fuente se menciona que “en los hoteles los hackeos son para obtener contraseñas y se puede entrar a los sistemas de las empresas” en el estudio se evidencia como los piratas informáticos utilizando sus capacidades en la informática roban las contraseñas para acceder a los datos personales de

los clientes de tal modo que perjudican directamente a la integridad de los huéspedes.

Cárdenas, J. (2015) en su investigación denominado “Metodología para mejorar la seguridad de la información y el funcionamiento del proceso administrativo, en la facultad de ciencias de la educación de la universidad estatal de Bolívar en el año 2013”, hace referencia a la seguridad de la información en las instituciones educativas y se establece que “no existen mecanismos que brinden seguridad a la información que se recepa. Se evidencia la poca cultura de mantener la seguridad de la información y el talento humano no domina el manejo de sistemas de información automatizados”. (p. 111)

En base a este concepto se puede evidenciar como el autor relaciona la falta de herramientas que brinden seguridad a la información con la poca cultura, y ciertamente es así, en las instituciones educativas lamentablemente no se incentiva en los docentes la capacitación en tecnología e innovación tal vez sea por descuido o simplemente por temor a su utilización, y es importante tener en claro que la tecnología es una arma de doble filo, es decir, si no se le da el uso y mantenimiento adecuado, se vuelve vulnerable al cometimiento de delitos que puede causar daños y perjuicios tanto para los estudiantes así como también para los docentes, puesto que puede provocar el robo de sus identidades, datos personales, hasta información financiera, e incluso plagio de proyectos e investigaciones. Es por ello que asegurar el entorno de las tecnologías de información permite proteger la integridad de los datos de las personas.

Flores, F. (2007) en su Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato da a conocer que “la implementación de políticas de seguridad informática, facilitan la administración de red, así como reducen errores de los usuarios por mal manejo en los computadores”. (p.23)

Así como se ha visto indispensable resguardar la información en los centros educativos, hoteles, la misma importancia es para las instituciones de salud, es así como frente a los riesgos observados en relación al robo de

información, la implementación de políticas es vital para proteger la información contra incidentes, así por ejemplo utilizando un buen antivirus se evita el contagio de virus que pueden provocar la pérdida de información, sumándose también software que contribuyen al aseguramiento de la información, en el estudio se evidencia como la adquisición de estas herramientas de seguridad han logrado un gran impacto positivo en relación al rendimiento y productividad de la institución.

Si bien es cierto el estudio se centra en las empresas del sector servicios reguladas por la Superintendencia de Compañías, en la investigación se considera necesario estudiar a las instituciones financieras reguladas por la Superintendencia de Economía Popular y Solidaria (SEPS). Por el mismo hecho de que en las instituciones de intermediación financiera se maneja dinero ajeno de los usuarios o socios, el tema de protección de información sean éstos datos personales de los usuarios o datos de la propia institución como la información contable o financiera, por todo lo mencionado las herramientas de seguridad y protección de datos en las Cooperativas de Ahorro y Crédito es el pilar fundamental para garantizar su credibilidad y confianza de los usuarios o socios. Algunos estudios realizados a este ramo tenemos:

Según Bermúdez, K. y Bailón, E. (2015) concluyen en su investigación denominado Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de servicios financieros, en el análisis realizado:

Refleja potenciales índices de riesgos, los cuales exponen a la información a daños, robo o modificaciones que pueden causar un impacto negativo dentro de las actividades del negocio. La implementación de controles de seguridad basados en la norma ISO/IEC 27001, les permite mejorar tres características importantes como son: la confidencialidad, integridad y disponibilidad de la información. (p.135)

En base al estudio realizado por el autor ciertamente identifica que las entidades financieras es el sector que mayor riesgo presenta frente a los ataques cibernéticos, en tal sentido es muy importante que en las

instituciones financieras implementen medidas de seguridad a la información de los usuarios y de la propia institución, anteriormente el autor recalca en la relevancia de implementar las normas ISO/IEC con el objetivo de saber cómo implantar, mantener y mejorar un sistema de gestión de seguridad de la información, lo que a su vez permitirá garantizar para el cliente servicios de calidad.

Según Sánchez, L. (2015) en su trabajo realizado sobre un Modelo de Gestión para el Desarrollo de Procesos de Seguridad en la Red de Datos de la Cooperativa de Ahorro y Crédito Guaranda Ltda., establece:

Un plan de seguridad informática de la Institución tendrá diversas áreas de aplicación, esto quiere decir que se subdividirá en planes de seguridad para software, para hardware, para redes, para servidores, para prevención de desastres, para respaldo de la información y más. La integración de todos los planes tecnológicos en diferentes aspectos, más las políticas de uso, se convierten en un modelo de gestión tecnológica que es el que dirigirá el rumbo institucional en el ámbito de las tecnologías. (p.117)

Así como el mundo globalizado va creciendo rápidamente, el mundo de los negocios lo hace también, y de allí surge la necesidad de proteger aún más la información de la entidad y de los clientes.

Como es de conocimiento la tecnología nos ayuda y facilita el trabajo en los diferentes ámbitos, de igual forma son herramientas vulnerables que estando en las manos equivocadas puede comprometer a la integridad y confiabilidad de la información de las entidades, por lo cual la empresa pierde credibilidad y obviamente los clientes se alejan, puesto que las personas al menos en una institución financiera lo primordial es la confianza que la institución brinda.

Se demuestra que las empresas de servicio como las de intermediación financiera presentan riesgos en las áreas que manejan información ya sea personal, contable o financiero, y para mitigar o reducir el riesgo de pérdida, o modificación de los datos, se requiere implementar controles de seguridad de la información, en este sentido el autor enfatiza en la importancia de una buena gestión tecnológica que básicamente es el conjunto de procesos que llevan a la planeación, organización y control de los sistemas de tecnología,

este conocimiento apoyará al personal en la decisión de adquirir alguna herramienta de seguridad y protección de datos visualizando la pronta recuperación de la inversión realizada por la entidad, y garantizando al cliente servicios de calidad.

Algunas herramientas y medidas de seguridad se muestran las claves de acceso, firewall físicos, respaldos, etc., e incluido también la capacitación al personal, en su conjunto permitirán prevenir los fraudes o el uso de información indebida.

Para concluir de los antecedentes presentados se evidencia como las empresas de actividades de alojamiento, de intermediación financiera, educación, salud y en general toda empresa de servicios requieren implementar herramientas orientadas a la seguridad y protección de datos, su adquisición no es un proceso fácil puesto que se requiere previamente un análisis del costo versus el beneficio de la inversión, lo que una empresa busca son productos buenos que realmente sean útiles para el giro del negocio, en este caso herramientas informáticas a menores costos pero con grandes beneficios para la entidad.

1.3. Planteamiento del problema

1.3.1. Macro Contextualización

A nivel mundial hay que considerar que las empresas están cada vez más interconectadas e integradas; lo que incrementa la probabilidad de que exista peligro en el manejo de su información, ya que se emplea la tecnología para compartir un gran volumen de datos con clientes, proveedores, socios y empleados.

Según estadísticas compartidas a Diario El Mundo (2015) cuyos datos fueron recopilados por la Compañía de Telecomunicaciones Intelfon a través de su marca Data Red indica que:

Existe un porcentaje alto de organizaciones, entre ellas el 53 %, que no realiza copias de seguridad, por otro lado el 32 % de las compañías considera que hacer respaldos no es eficiente y el 23 % de los administradores de tecnologías de la información cree que realizar respaldos no es necesario. Además, el 60 % de las empresas considera que no es importante tener un sitio de contingencia externo y

el 40 % de administradores de tecnologías no tiene el presupuesto para contratar un servicio de esta índole.

La seguridad informática se enmarca en un contexto mundial, pues la ciberdelincuencia crece desarrollando nuevas maneras de producir incidentes de ciberseguridad en todas las empresas alrededor del mundo sin embargo según las estadísticas presentadas anteriormente se puede observar que el tema de seguridad informática aun es débil principalmente para las empresas que son creadas recientemente y además ciertas empresas que se encuentran en el mercado no tienen los conocimientos o los recursos necesarios para proteger sus datos adecuadamente. Cabe destacar además los hechos noticiosos generados, en estos últimos años donde varias empresas fueron afectadas por los ciberataques en distintos países, casos muy recientes se puede mencionar el ataque informático a Hospitales y Centros Médicos del Reino Unido, así también se vieron afectados por ataques masivos un elevado número de empresas españolas, y la compañía privada de correos estadounidense FedEx.

Cabe mencionar también que muchos de los ataques informáticos se dieron lugar fácilmente por los inconvenientes que, “Aprovecharon los sistemas operativos desactualizados de empresas o instituciones en todo el mundo, especialmente en Rusia, Ucrania y Taiwán”, donde surgió estos incidentes según indica el analista de Malware de Avast. (Kroustek Jakub, 2017)

Por otro lado el cumplimiento regulatorio y la seguridad de la información son más estrictos en países de Estados Unidos, China y Europa por el mismo hecho que se encuentran más expuestos a los piratas informáticos y de igual forma son estos países donde tiene lugar el desarrollo de habilidades en métodos y técnicas de los piratas informáticos, quienes propagan ataques maliciosos en todo el mundo afectando la integridad de los datos en las empresas.

Según se indica en la página web de WeLiveSecurity, Editor (2017) menciona que:

La seguridad de los datos, en general, adquirirá un mayor peso, se espera que para 2020 un 60% de las organizaciones utilicen múltiples funcionalidades para asegurar su información, tales como aquellas para la prevención de pérdida de datos, de cifrado, y otras de auditoría y protección de base de datos.

La delincuencia cibernética actualmente representa una gran amenaza, por lo tanto las organizaciones alrededor del mundo cada vez más miran al tema de seguridad informática como un área en crecimiento para la inversión en seguridad de la información pues no se descarta la posibilidad de que alguna empresa cualquiera sea la actividad sufra o corra el riesgo de que su información sea tomada como rehén lo que significa para la víctima pérdidas económicas cuantiosas debido al costo monetario que involucra el valor de la información, además si se produce esta situación también se da lugar a la interrupción de actividades pues implica un obstáculo para acceder a la información, todo esto y más hechos tienen lugar a raíz de infiltraciones de piratas informáticos en entidades que hasta un cierto punto, parecían impenetrables en materia de seguridad física e informática, sin embargo actualmente han demostrado que son cada vez más el panorama de amenazas a la seguridad informática de las empresas, por lo cual estas deben adaptarse para anticiparse a los nuevos retos que a nivel mundial se presentan.

1.3.2. Meso Contextualización

Desde el punto de vista de países Latinoamericanos se destaca que el activo más importante de una organización es la información que tiene cada una de ellas, lo cual viene hacer un elemento sensible que se debe proteger debido al valor que representa para las empresas considerándose tan valioso como el funcionamiento mismo de la organización.

Según el artículo publicado por Chacón Krisia (2016) donde da a conocer datos de un estudio realizado Eset Security Report Latinoamérica 2016 indica que:

La investigación tomó en consideración 3.044 encuestas que fueron aplicadas en Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú y Venezuela. El país que más registra ataques por malware o códigos

maliciosos es Nicaragua (58%) y por el momento Costa Rica ocupa la séptima posición (45%).

En Latinoamérica la situación sobre seguridad informática es también compleja pues los riesgos y amenazas a los que se enfrentan las empresas en los últimos años viene aumentando y estas son evidentes pues en estudios realizados se da a conocer que ciertas empresas no tienen servicios de ciberseguridad, es decir que las empresas no saben protegerse ante un ciberataque, existen varias razones pero las más comunes implica el fantasma de la inversión, así también el desconocimiento del tema, por este motivo existen aún modelos de seguridad obsoletos lo que vuelve más atractivo para este tipo de delincuentes y una oportunidad para obtener la información, influencia y ventajas sobre sus contrarios donde las empresas más pequeñas llegan a ser más vulnerables, así claro ejemplo la campaña del ransomware WannaCrypt poderosos virus que se han propagado secuestrando fácilmente datos de los ordenadores infectados.

Según Ávila (2016) en su artículo menciona que:

El sector financiero es uno de los más vulnerables ante ataques informáticos, especialmente en los países latinoamericanos. Por ahora, Colombia se reporta como el tercer país más afectado en el último año y se revela que la seguridad informática no es una fortaleza, sino una debilidad.

Colombia es un país que tiene grandes inconvenientes en el tema de seguridad informática donde el principal foco de atención para los piratas informáticos son las instituciones financieras a pesar de que estas se ven obligadas a cumplir con estándares mínimos de seguridad, debido a su dependencia en la información aún enfrentan grandes desafíos para garantizar la protección de los datos, esto también implica el avance y el acceso a internet que ha tenido un gran auge en los últimos años volviéndose una herramienta indispensable para las empresas y este también se vuelve un punto clave para cometer este tipo de delitos por lo cual representa también grandes riesgos ya que constituye un camino que utiliza la ciberdelincuencia ante la privacidad de los datos, así mismo cabe mencionar que ahora las pequeñas y medianas empresas también se pueden ver afectadas de igual manera o quizá más que el resto de las

organizaciones pues no cuentan con los mecanismos necesarios para proteger su información.

En este contexto el estado de la inversión en seguridad informática en Latinoamérica según Bortnick (2010) indica que “en promedio las empresas asignan 5% del presupuesto de IT a la seguridad en donde del total del presupuesto en seguridad se distribuye así: 37% es abocado a personal, 25% al software, 20% al hardware, 10% a tercerización (outsourcing) y un 9% a consultoría” lo que es importante ya que cada componente constituye un sistema de gestión de la seguridad de la información sin embargo no es suficiente para estar a la vanguardia de los nuevos avances del cibercrimen por lo cual las organizaciones de la región ha sufrido ataques, donde el principal incidente es la fuga de información, considerándose a este tipo de interferencias como catastrófico ya que los delitos informáticos representa grandes pérdidas económicas para las empresas o simplemente para un país estos actos representan millones de dólares por esto al no poseer planes de respuestas el tema de seguridad y protección de datos se convierte en un tema que representa riesgo económico como competitivo para las mismas.

1.3.3. Micro contextualización

Desde una perspectiva micro se considera pertinente visualizar los hechos acontecidos en el Ecuador principalmente en las ciudades más grandes de nuestro país donde se produjo ciberataque en las empresas siendo un claro ejemplo al riesgo al que se encuentra expuesta la seguridad informática de la entidades cualquiera sea su actividad económica; es importante mencionar que esta investigación hace énfasis al análisis a nivel de Cotopaxi de aquellas empresas de servicios reguladas por las Superintendencia de Compañías, sin embargo debido a que estas entidades no tienen suficiente información en temas de herramientas de seguridad y protección de datos para el análisis se ha expandido la población enfocando a las Cooperativas de Ahorro y Crédito reguladas por la Superintendencia de Economía Popular y Solidaria, ya que son instituciones que están expuestas a posibles amenazas y actualmente advierten peligros que provienen del

exterior y del interior de las empresas, por lo cual la seguridad de la información se encuentra en riesgo.

Según Ortega (2015) en su artículo publicado en Diario el Comercio el 24 de enero, sobre el registro de ataques informáticos y robos de datos confidenciales en empresas ecuatorianas menciona que:

En Ecuador se propagó un virus denominado 'malware' mismo que avanzó y en cinco días penetró en los ordenadores de unas 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca. El programa maligno ingresó en las computadoras y encriptó archivos sensibles: documentos levantados en Word, Excel, Autocad. Una de las empresas atacadas perdió carpetas en las que se almacenaban datos del departamento de contabilidad.

Tras el ataque, en las máquinas ecuatorianas se desplegó una pantalla roja con una amenaza. "Tus archivos importantes fueron encriptados. Para obtener la clave y liberarlos, debes pagar USD 300 o una cantidad similar en otra moneda".

La seguridad y protección de datos actualmente es un tema de mucha relevancia, mismo que si no se trata con la debida importancia en las empresas las operaciones de estas posiblemente tienden a verse afectadas por la ciberdelincuencia u otro tipo de amenazas, claro es el ejemplo que vivieron ciertas empresas de Quito y Guayaquil, en este sentido cada vez son más los casos de empresas que sufren estos inconvenientes en las operaciones normales de su día a día, este tipo de delitos atenta contra el recurso más importante de toda empresa como es la información, ya que al ocurrir estos incidentes da lugar a que se infecten automáticamente cada uno de los ordenadores, ya que son virus que se propagan rápidamente cifrando datos y sin lugar a duda se convierten en un riesgo inminente para cualquier organización. Al verse en esta situación se procede a pagar cierta cantidad de dinero que pide el ciber-delincuente con el fin de tener de vuelta los datos sin embargo muchos son los casos en los que no se les devolvía la información respectiva produciéndose muchas veces hasta el quiebre de las empresas.

Cualquier empresa es un blanco potencial para dar lugar a que ocurran delitos informáticos, así como los ataques cibernéticos y la violación de datos que principalmente tienen fines vandálicos o económicos, por esto se ha considerado importante tratar en esta investigación el tema de análisis

Costo – Beneficio para conocer como contribuye este tipo de Herramientas a la seguridad de la información y con ello el desarrollo y competitividad de las empresas en nuestro país principalmente en Cotopaxi.

1.3.4. Árbol de problemas

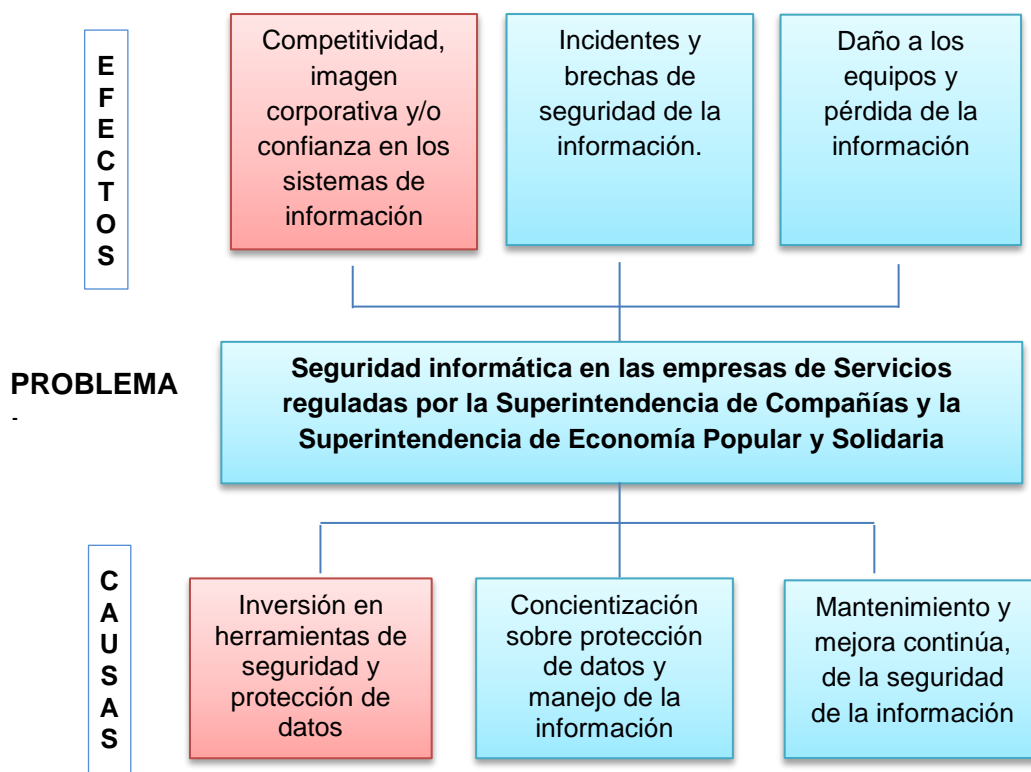


Figura 1. Árbol de problemas

1.4. 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?

1.5. Justificación

El desarrollo de este trabajo de investigación tiene como objetivo demostrar cuán importante puede ser el invertir en herramientas de seguridad y protección de datos, a través de un análisis de costo- beneficio aplicado a las empresas del sector servicios reguladas por la Superintendencia de Compañías en la provincia de Cotopaxi cabe mencionar que por motivo de información para analizar se ampliado la

población hacia las entidades reguladas por la Superintendencia de Economía Popular y Solidaria.

Además la investigación es conveniente debido a que actualmente el tema de seguridad informática en las empresas es un aspecto que está cada vez más expuesto a robos, modificación o eliminación de información, por ello la mayoría de las empresas de servicios pueden verse afectadas su imagen corporativa o incluso generar pérdidas económicas debido a la magnitud que representa la información, así también la investigación beneficia a las entidades de Cotopaxi que están dentro del sector de estudio y con los resultados obtenidos podrán tener un enfoque de lo que implica la inversión en seguridad.

Con esta investigación se busca analizar también el porcentaje que invierten las empresas de los distintos segmentos financieros y demás ramos del sector servicios en Herramientas de Seguridad y protección de datos.

Como propuesta al tema de estudio se creará un simulador para conocer el retorno de la inversión en seguridad de la información, previo a la identificación de los problemas detectados en cada caso de estudio, permitiendo que las empresas conozcan más sobre este tipo de inversiones, los costos, beneficios que implica asignar un porcentaje de presupuesto a la inversión en temas de seguridad.

1.6. Delimitación de la investigación

La presente investigación tiene como finalidad realizar un análisis costo-beneficio llevado a cabo con empresas de los diferentes ramos del sector servicios reguladas por la Superintendencia de Compañías y por la SEPS que utilizan herramientas de seguridad y protección de datos en la provincia de Cotopaxi, durante el periodo 2012-2016. En este caso la fuente de información contable-financiera es propiamente del sitio web del ente regulador y en algunos casos de la misma institución que forma parte del presente estudio.

1.7. Objetivos

1.7.1. 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.

1.7.2. Objetivos específicos

- 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.
- 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.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Fundamentación Teórica

2.1.1. Normas ISO/IEC 27000

La ISO 27000 es un conjunto de estándares que proporciona una guía para el desarrollo, implementación y mantenimiento de un sistema de gestión de la información utilizada en cualquier tipo de empresa u organización.

ISOTools (2015) destaca las siguientes normas pertenecientes a la familia de la ISO 27000:

2.1.2. ISO/IEC 27001

Es la norma principal de toda la serie ya que incluye todos los requisitos del Sistema de Gestión de Seguridad de la Información en las organizaciones, y además, nos da la información necesaria para la utilización del ciclo PHVA (viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés “Plan, Do, Check, Act”).

Esta norma internacional con enfoque en un SGSI, es explicado a través del ciclo de mejora continua, es así como en la fase de planificación se establecen las políticas, objetivos o procesos del SGSI, para la segunda fase se procede a su implementación, en la fase de verificar es necesario monitorear y revisar el sistema, y finalmente se establecen medidas correctivas o preventivas. En su conjunto garantizará la disponibilidad, confidencialidad e integridad de la información.

2.1.3. ISO/IEC 27002

Es un manual de buenas prácticas en la que se describen los objetivos de control y las evaluaciones recomendables en cuanto a la seguridad de la información. Esta norma no es certificable. En ella podemos encontrar 39 objetivos de control y 133 controles agrupados en 11 dominios diferentes.

Básicamente esta norma muestra recomendaciones sobre los controles aplicables para la seguridad de la información, independientemente del tamaño o tipo de empresa a la cual pertenezca, llevar a cabo buenas

prácticas en el manejo de la información, permite a la empresa disminuir los incidentes de seguridad, y a la vez aumentar su competitividad en el mercado.

2.1.4. Controles de ISO/IEC 27002

Según López, A. y Ruiz, J. (2012) La ISO/ICE 27002 es una guía de buenas prácticas la cual abarca un conjunto de 14 dominios, 35 objetivos y 114 controles aplicables a la Seguridad de la información de todo tipo de organización si bien no hace falta cumplir todos los controles pero si considerarlos para su posible aplicación, a continuación se describirá cada uno de ellos:

a. Políticas de Seguridad

Los controles dentro de este dominio hacen referencia a la importancia de establecer políticas adecuadas de seguridad mismas que deben estar aprobadas por la dirección, ser comunicadas a todos los niveles de la empresa, y de igual forma revisar oportunamente las políticas y actualizarlas de ser el caso.

✓ Conjunto de políticas para la seguridad de la información.

La dirección debe aprobar, publicar y comunicar las políticas de SI dentro (todos) y fuera (personas relevantes) de la entidad.

✓ Revisión de las políticas para la seguridad de la información

Las políticas de SI deben ser revisadas cada cierto tiempo de forma planificada.

b. Aspectos organizativos de la Seguridad de la Información

Los controles de este dominio buscan estructurar el marco de seguridad considerando una gestión eficiente en la asignación de roles, tareas, responsabilidades, asignación de políticas, implementación de la seguridad etc.

✓ **Asignación de responsabilidades para la seguridad de la información.**

La dirección debe asignar responsabilidades creando compromiso sobre la SI.

✓ **Seguridad de la información en la gestión de proyectos.**

Al llevar a cabo un proyecto es importante considerar la seguridad de la información.

✓ **Política de uso de dispositivos para movilidad.**

Adoptar políticas de seguridad que permitan el uso adecuado de informática móvil y telecomunicaciones.

✓ **Teletrabajo**

Medidas de seguridad para la protección de la información como resultado del teletrabajo.

c. Seguridad ligada a los recursos humanos

Los problemas de seguridad también tienen su origen dentro de la empresa y son a causa del error humano por tanto estos controles se enfocan en instruir e informar al personal desde su ingreso y de forma continua sobre la importancia que tiene las medidas de seguridad y la confidencialidad que deben manejar en el desarrollo de sus actividades.

✓ **Investigación de antecedentes**

De acuerdo a los requerimientos de trabajo los candidatos al empleo deben pasar por una verificación de antecedentes

✓ **Términos y condiciones de contratación**

En el contrato se debe especificar las obligaciones tanto del empleador como del trabajador en aspectos para la SI.

✓ **Responsabilidades de gestión**

Todos los involucrados en los procesos de gestión deben aplicar seguridad de la información de acuerdo con las políticas y procedimientos.

✓ **Concienciación, educación y capacitación en SI**

Todos quienes estén involucrados en las actividades de la empresa deben tener el entrenamiento apropiado en distintos aspectos para desempeñar su labor.

✓ **Cese o cambio del puesto de trabajo**

Asegurar las medidas necesarias asignando responsabilidades bien definidas para evitar fugas de información una vez que el empleado abandone o cambie su puesto de trabajo.

d. Gestión de activos

Estos controles buscan que la entidad tenga conocimiento exacto de los activos que posee en cuanto a recursos de información, recursos de software, activos físicos, servicios informáticos y de comunicaciones (iluminación, calefacción, energía eléctrica, etc.) y se enfoca también al tratamiento que debe darse a cada uno de estos con medidas adecuadas que protejan de las incidencias, fallas en la seguridad.

✓ **Inventario de Activos**

Se debe identificar claramente todos los activos de la entidad.

✓ **Propiedad de los activos**

Cada área es responsable de la información y los activos inventariados a su cargo.

✓ **Uso aceptable de los activos**

Para el uso adecuado de la información y los activos es necesario implantar regulaciones y demás medidas necesarias.

✓ **Devolución de los activos**

Una vez finalizado los acuerdos, contrato de empleo es obligatorio proceder a la devolución de los activos que estén en su posesión.

✓ **Directrices de clasificación**

Para la clasificación de la información se debe considerar la sensibilidad, criticidad, el nivel de importancia que representa a la entidad.

✓ **Etiquetado y manipulado de la información**

Considerando el esquema de clasificación se debe adoptar un procedimiento apropiado para el etiquetado y tratamiento de la información.

✓ **Manipulación de activos**

Acorde al esquema de clasificación de la información se debe implantar y desarrollar procedimientos para el manejo adecuado de los activos.

✓ **Gestión de soportes extraíbles**

Considerando el esquema de clasificación adaptado se debe se deberían establecer procedimientos para la gestión de medios informáticos removibles.

✓ **Eliminación de soportes**

Una vez que los medios de soporte ya no sean requeridos se debe proceder a la eliminación de forma segura a través de procedimientos formales.

✓ **Soportes físicos en tránsito**

Cuando los medios que contengan información procedan al transporte fuera de la organización se debe proteger contra el acceso no autorizado, y manipulación de la información.

e. Control de Accesos

Este dominio surge de la necesidad de establecer un sistema de restricciones a las bases de datos mediante control de accesos ya que no todas las personas de una empresa necesitan acceder a toda la base de datos para desempeñar sus funciones de acuerdo a esto dependiendo de los roles se establecerá límites en los accesos.

✓ **Política de control de accesos**

Establecer políticas formales sobre el control de accesos considerando las necesidades de seguridad de la información para la empresa

✓ **Control de acceso a las redes y servicios asociados**

Establecer un sistema de restricciones para usuarios no autorizados a los accesos a redes y servicios de red.

✓ **Gestión de altas/bajas en el registro de usuarios**

Gestionar el registro de nuevos y la eliminación de usuarios con el fin de habilitar la asignación de derechos de acceso.

✓ **Gestión de los derechos de acceso asignados a usuarios**

Se realiza con el fin de asignar o revocar derechos de acceso

✓ **Gestión de los derechos de acceso con privilegios especiales**

Se deberían restringir y controlar este tipo de asignación de accesos.

✓ **Gestión de información confidencial de autenticación de usuarios**

El usuario debe seguir un proceso para tener acceso a la información confidencial

✓ **Revisión de los derechos de acceso de los usuarios**

Se debe establecer un control regular del derecho de acceso a los usuarios a los distintos activos.

✓ **Retirada o adaptación de los derechos de acceso**

La finalización del empleo, o por motivos de cambios del trabajo se debe retirar todos los derechos de acceso a la persona involucrada.

✓ **Uso de información confidencial para la autenticación.**

En el proceso de autenticación los usuarios deben seguir las buenas prácticas de seguridad.

✓ **Restricción de acceso a la información**

Tomar medidas de restricción de acceso a la información a los usuarios y el personal de mantenimiento.

✓ **Procedimientos seguros de inicio de sesión**

El acceso a los sistemas y aplicaciones deben ser controlados por un procedimiento seguro de inicio de sesión.

✓ **Gestión de contraseñas de usuario**

Se realiza con el fin de garantizar y asegurar contraseñas de calidad

✓ **Uso de herramientas de administración de sistemas**

Se debería restringir y tener un control minucioso en el uso de herramientas de administración del sistema

✓ **Control de acceso al código fuente de los programas**

El acceso al código fuente de las aplicaciones software debe ser restringido.

f. Cifrado

La importancia de este dominio se dirige a garantizar la protección de la autenticidad, confidencialidad e integridad de la información sensible o crítica a través del uso de sistemas y técnicas criptográficas.

✓ **Política de uso de los controles criptográficos**

Estas políticas permitirán regular el uso de Controles criptográficos

✓ **Gestión de claves**

Se debe desarrollar e implantar políticas para la gestión de claves criptográficas durante todo su ciclo de vida

g. Seguridad física y ambiental.

La seguridad física y ambiental es muy importante y estos controles buscan reducir los riesgos de daños e interferencias a la información y a las

operaciones de la organización definiendo perímetros y áreas de seguridad, además las medidas necesarias para la seguridad de los equipos.

✓ **Perímetro de seguridad física**

Se realiza con el fin de proteger las áreas e instalaciones que contienen y procesan información sensible o crítica.

✓ **Controles físicos de entrada**

Garantizar el acceso solo al personal autorizado a las áreas seguras

✓ **Seguridad de oficinas, despachos y recursos**

Se debe establecer sistemas de seguridad para todas las instalaciones de la empresa.

✓ **Protección contra las amenazas externas y ambientales**

Permite el correcto funcionamiento de los equipos de procesamiento

✓ **El trabajo en áreas seguras**

Se debe establecer procedimientos para el desarrollo de actividades en áreas seguras

✓ **Áreas de acceso público, carga y descarga.**

Las áreas seguras deben estar alejadas de las zonas de acceso público.

✓ **Emplazamiento y protección de equipos**

Los equipos se deben ubicar en zonas seguras para reducir los riesgos de amenazas y peligros ambientales.

✓ **Instalaciones de suministro**

Los equipos de apoyo se deben inspeccionar de forma regular protegiendo a los equipos contra posibles fallos eléctricos y suministros de energía

✓ **Seguridad del cableado**

El cableado que transporte datos o soporten servicios de información deben ser protegidos contra posibles interceptaciones o daños.

✓ **Mantenimiento de los equipo**

El mantenimiento garantiza la disponibilidad e integridad de los equipos

✓ **Salida de activos fuera de las dependencias de la empresa**

Se requiere previa autorización para poder movilizar los activos

✓ **Reutilización o retirada segura de dispositivos de almacenamiento.**

Los equipos deben contar con medios de almacenamiento para garantizar que datos sensibles se hayan extraído y sobrescrito de forma segura antes de su eliminación o reutilización

✓ **Equipo informático de usuario desatendido**

Los usuarios deben asegurar que los equipos no supervisados disponen de protección adecuada

✓ **Política de puesto de trabajo despejado y bloqueo de pantalla**

La documentación en papeles y medios de almacenamiento extraíbles deben guardarse de modo que no pueda manipularse o divisarse por otros usuarios no autorizados de igual forma los monitores no deben mostrar información.

h. Seguridad en la operativa

La información y las instalaciones del proceso de información deben tener un grado de protección muy grande con el fin de evitar el acceso físico no autorizado, posibles interferencias, estar protegidos contra malware, hacer frente la pérdida de datos, además es importante generar evidencia de todos los eventos relacionados con la SI, se requiere también mediante auditorias

técnicas verificar el cumplimiento de las normas, procedimientos y controles establecidos.

✓ **Documentación de procedimientos de operación**

Cuando se considere necesario se debe documentar los procedimientos de las actividades operacionales garantizando el buen funcionamiento de los recursos.

✓ **Gestión de cambios.**

Controlar los diferentes cambios que se presentan en los sistemas o en las instalaciones y que de alguna manera afectan a la seguridad de la información.

✓ **Gestión de capacidades.**

Monitorear las capacidades de los sistemas de información y encontrar las futuras demandas de capacidades que requieran los sistemas en función de las exigencias de las operaciones de la empresa.

✓ **Separación de entornos de desarrollo, prueba y producción.**

Esta separación de entornos ayuda principalmente a evitar el acceso no autorizado o incluso de cambios en el sistema.

✓ **Controles contra el código malicioso.**

Los códigos maliciosos hacen que el sistema sea vulnerable a robos, daños, pérdidas o modificaciones de la información, por tal razón es importantes establecer controles de detección y prevención ante los posibles malware, sin olvidar los controles de recuperación en caso de generarse fugas de información, por otro lado el personal debe tomar consciencia a la hora de abrir o descargar archivos que no sean tan seguros, este es un complemento para lograr la efectividad de la implementación de controles.

✓ **Copias de seguridad de la información.**

Una vez que se determine los procedimientos Backup o simplemente copias de seguridad a la información y los procedimientos de recuperación, es necesario efectuar pruebas constantes para verificar su grado de efectividad.

✓ **Registro y gestión de eventos de actividad.**

Es necesario contar con los registros de eventos anteriores o presentes que afectan a la seguridad de la información.

✓ **Registros de actividad del administrador y operador del sistema.**

Los registros deberán ser revisados regularmente y deberán ser protegidos especialmente de modificaciones o accesos no autorizados a la información.

✓ **Sincronización de relojes.**

Los sistemas de información deberán contar con una sincronización única de tiempos.

✓ **Instalación del software en sistemas en producción.**

Una correcta instalación del software requiere de algunos procedimientos de control por ejemplo se puede mencionar que una instalación debe ser efectuada por el personal autorizado, así también se debe realizar pruebas empezando desde los sistemas menos críticos, además de informar a los usuarios antes de efectuar los cambios en el sistema.

✓ **Gestión de las vulnerabilidades técnicas**

Las técnicas inadecuadas que son utilizadas en los sistemas lo vuelven vulnerable frente a la seguridad de la información, por tal razón es necesario tener conocimiento sobre las vulnerabilidades técnicas ayudando a detectar el impacto en la organización y así también permite establecer medidas para tratar los riesgos provocados.

✓ **Restricciones en la instalación de software**

Se debe implementar las reglas que el usuario debe tomar en cuenta al momento de instalar un software.

✓ **Controles de auditoría de los sistemas de información.**

Con el objetivo de evitar interrupciones en el sistema de información el auditor deberá elaborar y coordinar tiempos con los usuarios sobre su plan de actividades con respecto a la verificación del sistema

i. Seguridad en las Telecomunicaciones

El intercambio de información por lo general es realizado a través de redes informáticas, y más aún cuando se maneja información confidencial, es necesario establecer medidas para protegerla de usos indebidos, modificaciones o robos de información de terceras personas.

✓ **Controles de red.**

Una red es un conjunto de equipos conectados entre sí para compartir información, de ahí surge la importancia de resguardar la información a través de una buena administración y mecanismos de control de la red.

✓ **Mecanismos de seguridad asociados a servicios en red.**

Los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de los servicios de la red necesariamente deberán estar escritos en los acuerdos de servicios entre proveedor y cliente.

✓ **Segregación de redes**

Es importante separar las redes según grupos de usuarios, servicios y sistemas de información.

✓ **Políticas y procedimientos de intercambio de información.**

Disponer de políticas y procedimientos que guíen el intercambio de información a una organización externa, así también establecer los controles necesarios para resguardar la información de la empresa.

✓ **Acuerdos de intercambio.**

Los acuerdos serán exclusivos a la seguridad de la información que se realizarán únicamente entre la empresa que emite la información y las partes externas que receptorán la información

✓ **Mensajería electrónica.**

Se refiere a la información que se transfiere de ordenador a ordenador sin la utilización de papel.

✓ **Acuerdos de confidencialidad y secreto.**

Es importante tener conocimiento sobre los requisitos necesarios a la hora de establecer acuerdos de confidencialidad y no divulgación de la información, con el fin de evitar fugas de información.

j. Adquisición, desarrollo y Mantenimiento de los sistemas de información.

Los sistemas que almacenan y procesan información sensible de una organización, desde su diseño hasta su eliminación, deben incluir requisitos que deberán cumplir tanto los desarrollos propios de la empresa como los realizados por servicios externos, y así resguardar la información contenida en los sistemas.

✓ **Análisis y especificación de los requisitos de seguridad.**

Es imprescindible contar con los requisitos de seguridad de información, requisitos de nuevos o mejoras en los sistemas de información.

✓ **Seguridad de las comunicaciones en servicios accesibles por redes públicas.**

Para evitar especialmente los fraudes

✓ **Protección de las transacciones por redes telemáticas.**

Las redes telemáticas permiten la comunicación entre personas por lo que se requiere protegerse en especial de las divulgaciones de información no autorizadas.

✓ **Política de desarrollo seguro de software.**

Es necesario contar con políticas que guíen el desarrollo del software dentro de la organización de forma segura.

✓ **Procedimientos de control de cambios en los sistemas.**

Desde la concepción hasta la destrucción del sistema de información se generan cambios por lo que se requiere procedimientos de control.

✓ **Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.**

Si se ha realizado cambios en el sistema operativo es necesario examinar y comprobar que las aplicaciones funcionen correctamente disminuyendo considerablemente los riesgos de la seguridad de la información.

✓ **Restricciones a los cambios en los paquetes de software.**

Cambiar los paquetes de software no es aconsejable, pero en caso de realizarlo, únicamente se efectuaran los cambios que realmente sean indispensables.

✓ **Uso de principios de ingeniería en protección de sistemas.**

Por ejemplo principios básicos de confiabilidad, disponibilidad e integridad de la información

✓ **Seguridad en entornos de desarrollo.**

Establecer medidas de seguridad física en las áreas destinadas para el desarrollo de los sistemas de información.

✓ **Externalización del desarrollo de software.**

Cuando se haya externalizado el desarrollo de un software necesariamente la empresa solicitante deberá monitorear cada una de las actividades que se realicen.

✓ **Pruebas de funcionalidad durante el desarrollo de los sistemas.**

Las pruebas de funcionalidad son realizadas para garantizar que el sistema de información sea confiable, y que cumpla con las especificaciones acordadas además de las expectativas del usuario.

✓ **Pruebas de aceptación.**

Las pruebas de aceptación son necesarias cuando la empresa desea implementar nuevos sistemas de información.

✓ **Protección de los datos utilizados en pruebas**

Es necesario elegir, cuidar y controlar los datos o información crítica utilizada en pruebas.

k. Relaciones con Suministradores

En caso de que una empresa contrate proveedores y tomando en cuenta que son conocedores de la información de la empresa, es necesario establecer medidas que garanticen la seguridad de la información, y por ende sea satisfactorio para las empresas con los servicios entregados por los proveedores o suministradores.

✓ **Política de seguridad de la información para suministradores.**

Las empresas proveedoras de herramientas informáticas deberán acatarse a las políticas de los usuarios sobre la seguridad de la información

✓ **Tratamiento del riesgo dentro de acuerdos de suministradores.**

Se debe controlar el acceso a la información por parte de los proveedores.

✓ **Cadena de suministro en tecnologías de la información y comunicaciones.**

La cadena de suministros de servicios y productos de tecnología, engloba procesos, personas, infraestructura, por ello la necesidad de

conocer los riesgos que podrían suscitarse y que al mismo tiempo destruyen la relación cliente – proveedor.

✓ **Supervisión y revisión de los servicios prestados por terceros.**

Debe ser efectuado regularmente.

✓ **Gestión de cambios en los servicios prestados por terceros.**

Las políticas de seguridad son una guía efectiva para aplicar correctamente los cambios a los servicios adquiridos por los proveedores de tecnologías de información.

I. Gestión de Incidentes

Los eventos de inseguridad e incluso los puntos débiles de los sistemas de información deben comunicarse entre el personal que le corresponde llevar a cabo acciones correctivas.

✓ **Responsabilidades y procedimientos.**

Al disponer de las responsabilidades y procedimientos para manejar las debilidades con respecto a la seguridad de la información, nos permite generar prontas y eficaces respuestas frente a los incidentes de información.

✓ **Notificación de los eventos de seguridad de la información.**

En caso de detectarse eventos que afecten a la seguridad de la información deberán ser comunicados inmediatamente a los empleados, contratistas y terceros.

✓ **Notificación de puntos débiles de la seguridad.**

Los empleados así como también los contratistas deben estar al tanto de las debilidades de seguridad que comprometen al sistema informático.

✓ **Valoración de eventos de seguridad de la información y toma de decisiones.**

Es necesario evaluar los eventos de seguridad de la información para determinar el nivel de impacto hacia la empresa.

✓ **Respuesta a los incidentes de seguridad.**

Para generar prontas y eficaces respuestas frente a los incidentes informáticos se requiere de los procedimientos establecidos en relación a la seguridad de la información.

✓ **Aprendizaje de los incidentes de seguridad de la información.**

La capacitación y la experiencia en incidentes informáticos es el punto clave para disminuir en el futuro posibles incidentes de seguridad de la información.

✓ **Recopilación de evidencias.**

La persona que es responsable de un incidente informático se enfrenta a acciones legales y de ahí surge la importancia de recopilar y preservar la información que sirve como evidencias del acto ilícito cometido.

m. Aspectos de la SI en la Gestión de la Continuidad de Negocio

La información debe ser protegida o recuperada cuando las actividades de la empresa se vean afectadas o interrumpidas después de un acontecimiento negativo.

✓ **Planificación de la continuidad de la seguridad de la información.**

Establecer procesos de gestión de continuidad de la seguridad de información durante las situaciones desagradables.

✓ **Implantación de la continuidad de la seguridad de la información.**

Es importante que las empresas implementen procedimientos y los controles necesarios de seguridad de la información en caso de producirse situaciones desagradables o adversas.

✓ **Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**

Es un punto indispensable, ya que permite determinar si los controles pese a las situaciones críticas aún tienen la capacidad de proteger la

información, caso contrario se deberá establecer nuevos controles que cubran la necesidad de resguardo de información

✓ **Disponibilidad de instalaciones para el procesamiento de la información.**

Se refiere básicamente a la redundancia de la información, es decir se almacenan los mismos datos en diferentes lugares.

n. Cumplimiento

Todo sistema de información que garantice su credibilidad, está sujeta a normativas y términos contractuales que deberán ser cumplidas por las partes involucradas.

✓ **Identificación de la legislación aplicable.**

Es necesario identificar, documentar y mantener actualizada estatutos, normativas y obligaciones contractuales para cada sistema de información.

✓ **Derechos de propiedad intelectual (DPI).**

Es importante utilizar software original, porque son más seguros para los usuarios, están aún más protegidos contra los ataques informáticos, a esto se suma también la importancia de contar con la documentación actualizada de legislaciones, normativas y contratos en relación a la propiedad intelectual.

✓ **Protección de los registros de la organización.**

Los registros de la organización deberán ser protegidos contra robos, modificaciones, destrucción, etc.

✓ **Protección de datos y privacidad de la información personal.**

En las normativas se establece lo indispensable de proteger los datos o información personal, y así garantizar la integridad de la persona.

✓ **Regulación de los controles criptográficos.**

Los controles criptográficos son básicamente códigos secretos que impiden el acceso a personas no autorizadas.

✓ **Revisión independiente de la seguridad de la información.**

Se refiere a que necesariamente se debe revisar los procedimientos, políticas, controles y demás a los que cada empresa está sujeta.

✓ **Cumplimiento de las políticas y normas de seguridad.**

La dirección de la empresa será el encargado de velar por el cumplimiento de las políticas y normas de seguridad.

✓ **Comprobación del cumplimiento.**

Revisar regularmente que los sistemas de información cumplan con las políticas y normas de seguridad.

2.1.5. ISO/IEC 27003

“Es un manual para implementar un Sistema de Gestión de Seguridad de la Información.”

La ISO/IEC 27003 proporciona una orientación práctica desde la generación o diseño hasta la propia implementación de un SGSI

2.1.6. ISO/IEC 27004

“En este estándar se especifican las técnicas de medida y las métricas que son aplicables a la determinación de la eficacia de un Sistema de Gestión de Seguridad de la Información y los controles relacionados.”

Esta norma establece la importancia de contar con procesos de medición que permitan evaluar el resultado del cumplimiento y el rendimiento de un SGSI, esto permite a las empresas proteger los sistemas de información, generando respuestas frente a las amenazas detectadas.

2.1.7. ISO/IEC 27005

“Esta normativa establece las diferentes directrices para la gestión de los Riesgos en la Seguridad de la Información.”

Es indispensable realizar un análisis de los riesgos asociados a los activos de la información, puesto que dicho análisis permite identificar las amenazas que permanentemente están expuestos los sistemas de información.

2.1.8. ISO/IEC 27006

“Este estándar especifica todos los requisitos para lograr la acreditación de las entidades de auditoría y certificación de Sistema de Gestión de Seguridad de la Información.”

En definitiva esta norma establece los requisitos necesarios a cumplir por parte de las organizaciones encargadas de las auditorías y certificaciones en concordancia con la gestión de la seguridad de la información, con el fin de garantizar su credibilidad ante las empresas que buscan una certificación.

2.2. Marco conceptual

2.2.1. Seguridad informática

“La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable” (Aguilera, 2010, pág. 9).

El ser humano en el transcurso de los años ha desarrollado grandes avances tecnológicos situando a la sociedad actual en un mundo de tecnología. La seguridad informática por los años cincuenta cuando aparecieron los primeros ordenadores no era un tema que plantease problemas a los administradores de sistemas ni empresarios, entonces la seguridad informática más “*Se basaba ante todo en una seguridad física (acceso físico al ordenador) y sólo especialistas cualificados podían controlar esas enormes máquinas, previniendo así la mala conducta de un trabajador malintencionado*” (Asensio, 2006, pág. 8).

Sin embargo, con el paso del tiempo estas máquinas fueron tomando gran relevancia dentro del ámbito doméstico y empresarial permitiendo automatizar los procesos dependiendo de tal modo para realizar sus trabajos, entorno a esto el mayor miedo en esos años era que algún virus

infecte el disquete lo cual hacia que personas pierdan mucho tiempo y dinero cabe mencionar que el tipo de amenazas al que se enfrentaban no producía efectos nada comparados a los que tenemos ahora. En los años 80 se dio lugar a un gran avance y los ordenadores personales a través del dispositivo módem comenzaron a comunicarse entre sí dando lugar a varias oportunidades en distintos ámbitos como el empresarial, pero esto a la vez daba lugar a una *“Disminución en la seguridad informática, al exponer a equipos y redes completas a grandes ataques, desde virus a intrusiones malévolas”* (Asensio, 2006, pág. 9)

De esa forma, muchas empresas tuvieron cuantiosas pérdidas económicas debido al primer gusano informático que se activó el 22 de noviembre de 1998 cuyo autor fue Robert Norris, a partir de estos sucesos día a día se presentan nuevos retos que nos impone la inseguridad por tanto las empresas actualmente ya no solo deben preocuparse por proteger físicamente sus sistemas sino que además establecer un cierto nivel de seguridad como conjunto de medidas preventivas y reactivas que contribuyan a proteger y resguardar la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos que resultan de las operaciones propias de las empresas.

Hay que considerar que al hablar de seguridad de la información es una inversión que nace de las necesidades propias de cada institución, que se hace necesario de acuerdo al procesamiento de datos que se genere estableciendo en base a ello y su importancia múltiples niveles de protección ya que la seguridad informática implica el software, la base de datos, metadatos, archivos y todo lo que la entidad valore.

2.2.2. Objetivos de la seguridad de la información

El propósito de la seguridad de los sistemas de información pretende que una empresa cumpla con todos sus objetivos implementando sistemas que tengan una especial atención y consideración hacia los riesgos relativos a las TIC de la organización, socios, clientes; etc.

Como señala Areitio (2008) los principales objetivos de la seguridad de la información son:

- **Disponibilidad y accesibilidad:** este objetivo pretende que el volumen de datos con los que trabaja una entidad o cualquier persona solo sea accesible para aquella que tenga autorización es decir indispensablemente debe ser un usuario autorizado, mientras que la disponibilidad se refiere a que la información va estar al alcance de los usuarios puede ser solo para su análisis pero estos no podrán ser manipulados, modificados o causar algún daño a la base de datos ya que no tienen el acceso pertinente.
- **Integridad:** Es el estado en donde la información por ningún motivo debe ser alterada, esto se refleja en dos facetas, en donde la primera se refiere a la integridad de los datos mismos que deben tener la cualidad de estar completo mientras se almacenan, procesan o transmiten y la segunda se refiere a la integridad del sistema que pretende que realice sus funciones de forma deseada garantizando que la información sea inalterada.
- **Confidencialidad de datos y de la información del sistema:** mediante este objetivo se busca garantizar que la información de carácter privado no sea revelada a usuarios que no tienen la autorización correspondiente, por lo tanto los datos almacenados deben estar protegidos de modo que se requerirán de accesos previos para poder ser revelados.
- **Responsabilidad a nivel individual (registros de auditoria):** Este objetivo busca que una entidad sea la responsable de tomar acciones únicas que le permitan cumplir con una adecuada seguridad de la información, muchas veces esto responde a un requisito de la política de la organización, además soporta el no repudio que se refiere a que no se puede negar un mensaje transmitido, así también la prevención y la prevención de intrusiones entre otras actividades.

- **Confiabilidad (aseguramiento):** busca garantizar que el sistema y la información que se procesa estén completamente protegidos, cuya probabilidad de que las medidas de seguridad funcionen de forma prevista sin ningún incidente estableciendo así la base de la confianza. (p.3)

2.2.3. Importancia de la seguridad de la información

Actualmente la mayoría de empresas dependen en gran magnitud de la información de modo que si su base de datos está expuesta podría darse lugar a la pérdida de la misma, por ello también es que hablar de seguridad es importante pues abarca una dimensión inimaginable en todos los ámbitos y esta necesidad nace de los distintos riesgos a los que se encuentra expuesta especialmente para las empresas es de vital importancia para su supervivencia, por ejemplo las grandes instituciones financieras dependen absolutamente del gran volumen de datos que generan sus operaciones normales y por el valor que representa realizan grandes inversiones en herramientas de seguridad y protección de datos pues las violaciones de seguridad informática de ser el caso produciría problemas muy serios y costosos, por esta razón para los directivos en una entidad no debe pasar por alto la gestión de la seguridad de la información.

2.2.4. Entidades implicadas en la seguridad y protección de la información

Según menciona Areitio (2008) quienes intervienen en el ámbito de la seguridad y protección de datos son las siguientes entidades o personas involucradas en los sistemas de información así tenemos:

- Desarrolladores de software
- Fabricantes de productos
- Integradores de datos en el sistema
- Compradores que pueden ser organizaciones o usuarios finales
- Organizaciones de evaluación de la seguridad, como certificadores de sistemas, evaluadores de productos o acreditadores de operación.
- Administradores de sistema y de seguridad
- Terceras partes confiables (TTP) como son las autoridades de certificación, fedatarios electrónicos con servicio de firma electrónica avanzada y sellado temporal
- Consultores u organizaciones de servicio, por ejemplo servicios de externalización de la gestión de la seguridad (pp.4, 5).

2.2.5. Datos

En informática se conoce como el conjunto de caracteres que pueden ser números, letras, símbolos u otras formas de representación que están listos para ser procesados por el ser humano y algún medio digital.

2.2.6. Información

Resulta del procesamiento de los datos que dan lugar al conocimiento lo que ayuda a la toma de decisiones.

a. Clasificación de la Información

Cada empresa es responsable de clasificar la información que generan de acuerdo a los criterios más apropiados que consideren cada uno de ellos, tomando en cuenta cuán sensible y crítica puede representar, pues es un activo muy importante que necesita un nivel adecuado de protección por lo tanto cada entidad debe adaptar reglas para dar protección a las diferentes categorías de información, estos niveles dependen y van acorde al tamaño que representa la organización, de esta forma además se pueda asignar a los usuarios responsabilidades con la información acorde a los permisos y accesos que tengan dependiendo de sus funciones y competencias dentro de la empresa.

La forma más habitual de clasificar la información puede darse lugar basándose en el criterio de confidencialidad, sin embargo a continuación se mostrara cinco niveles de información teniendo en cuenta los tres atributos de calidad (Confidencialidad, Integridad y Disponibilidad), esta clasificación según la investigación de Sosa J. (2012) pretende adaptarse a la mayoría de las empresas así tenemos los siguientes niveles:

- **Pública:** es la información al cual tienen acceso todas las personas es decir la información se encuentra disponible tanto para personas internas como externas a la organización.
- **Uso interno:** se refiere a la información al cual tienen acceso solo los empleados de la empresa, por lo tanto tienen un nivel bajo de confidencialidad.

- **Privada:** esta información tiene un nivel medio de confidencialidad, por lo tanto solo estará disponible para personas autorizadas.
- **Reservada /secreta:** se da este nivel a la información que incrementa su grado de sensibilidad por lo tanto tienen un grado más alto de seguridad.
- **Altamente reservada/ Súper secreta:** es la información de alta importancia que solo estará disponible y a la cual podrán acceder personas que ejerzan cargos de alto rango dentro de la empresa. (p. 30)

2.2.7. Herramientas de seguridad

Las herramientas de seguridad y protección son mecanismos que ayudan a resguardar la seguridad de la información de la empresa tomando en cuenta que cada vez más cantidad de información se encuentra en formato electrónico, en torno a esto actualmente existen varias soluciones en el mercado que ofertan distintos mecanismos de seguridad como antivirus, software especializados que ayudan a combatir la ciberdelincuencia, cabe considerar que estas herramientas dependen de cada sistema de información, de su función, de la importancia de los datos que se procesan dentro de la entidad y de las posibilidades económicas de las empresas, cabe indicar que estas herramientas pueden ser físicas y lógicas que pretenden detectar ataques al sistema y de esa forma asegurar que los servicios de seguridad queden cubiertos.

A continuación se indica de forma general las herramientas de seguridad y protección de datos, cabe indicar que cada uno de estos ofrece un sin número de alternativas de solución distintas acorde a la necesidad propia de las empresas.

En base al texto de Seguridad informática de Aguilera (2010) definimos las siguientes herramientas de seguridad lógica y seguridad física así tenemos:

a. Mecanismos de Seguridad lógica

Tienen como propósito proteger digitalmente la información de manera directa mediante barreras y procedimientos que resguarden el acceso a los datos, procesos y programas, proporciona seguridad en el uso de software y los sistemas, de esta forma solo se permite el acceso ordenado y autorizado de los usuarios a la información de la entidad.

- **Control de acceso:** funciona a través de usuarios y contraseñas y permite controlar y administrar el acceso para resguardar la información confidencial restringiendo la cantidad de usuarios y procesos con acceso permitido.
- **Cifrado de Datos** (encriptación): Los datos se vuelven ilegibles con una clave especial creada mediante un algoritmo de encriptación, para poder utilizar la información original, la información debe pasar por un proceso de descifrado de este modo si los datos son interceptados no podrán ser leídos mientras no se introduzca la clave del descifrado.
- **Antivirus:** este mecanismo previene y evita la entrada de virus y demás programas maliciosos, permite además en caso de contagio la eliminación y reconstrucción de los archivos y las áreas infectadas del sistema, sin embargo el antivirus no puede detener o detectar todo tipo de malware debido al constante desarrollo de los atacantes cibernéticos.
- **Cortafuegos:** (firewall): es un dispositivo que permite controlar el acceso a la red de manera que deniegan o restringen el acceso al sistema de acuerdo a una política de seguridad establecida y de esa forma permite las comunicaciones autorizadas además los firewall pueden ser implementados tanto en el hardware o software o de forma mixta.
- **Firma digital:** es una firma realizada con códigos matemáticos cifrados y se utiliza para autenticar información digital como documentos, correos electrónicos etc., identificando de forma segura

al emisor del mensaje y si esta información no ha sido alterada después del envío hasta llegar al receptor

- **Certificados Digitales:** permiten llevar a cabo trámites con otras entidades por lo tanto aquellos documentos son autorizados por una entidad autorizadora certificada que garantiza “que una persona o entidad es quien decide ser, avalada por la verificación de su clave pública”. (p.13)

b. Mecanismo de Seguridad Física

Son aquellos mecanismos cuyo objetivo es proteger físicamente cualquier recurso del sistema (y por tanto indirectamente a la información) es decir actúa contra peligros al cual pueden estar expuesto el hardware o cualquier medio de almacenamiento de datos.

- **Respaldo de Datos:** Consiste en realizar copias de seguridad de la información importante del sistema en otro medio y en lugar seguro con el objetivo de poder recuperarlas en caso de pérdida de la información. Hace referencia al criterio de disponibilidad.
- **Dispositivos físicos de protección:** hace referencia aquellos mecanismos como pararrayos, cortafuegos por hardware, alarma contra intrusos, detectores de humo y extintores, sistemas de alimentación interrumpida o mecanismos de protección contra instalaciones de igual forma para las personas, un mecanismo de acceso restringido a las instalaciones. (p.p. 17,18)

A parte de estas herramientas mencionadas anteriormente también existe otra forma de brindar seguridad a la información de una empresa y se lo hace a través del:

- **Servicio de externalización (outsourcing en seguridad):** consiste en un servicio externo especializado en protección y seguridad informática quien se encarga de la monitorización y gestión de vulnerabilidades y demás ciber-ataques a los que se enfrentan hoy en día las organizaciones, por lo tanto estas empresas especializadas a

través de un centro de datos protegen y analizan la información de la entidad quien la contrato ofreciendo los mayores niveles de experiencia en el área de TI.

2.2.8. Análisis y gestión de riesgos en un sistema informático

Gómez, A. (2011) establece que “El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático causando un determinado impacto en la organización”

El riesgo es básicamente que una vulnerabilidad del sistema informático pueda permitir la entrada a las amenazas causando daños o pérdidas económicas a la empresa, por tanto en la gestión de riesgos se empieza con la identificación de amenazas y vulnerabilidades, adicional de un análisis del nivel de impacto hacia la empresa, por último es necesario implementar medidas de seguridad que permitan mitigar el riesgo e impedir que cause incidentes de seguridad.

a. Amenazas

La amenaza según Gómez, A. (2011) “*puede ser un evento accidental o intencionado que ocasione algún daño en el sistema informático*”, ocasionando pérdidas económicas significativas, y desconfianza de los clientes hacia la empresa.

Se distingue los siguientes tipos de amenazas:

- **Amenazas naturales:** son eventos propios de la naturaleza que pueden causar efectos negativos en la operatividad de la empresa, es así por ejemplo que una inundación, incendio, fallo eléctrico muy probablemente afectará a los activos de la información.
- **Amenazas de agentes externos:** son producidos por personas ajenas a la institución con la intención de sacar provecho económico e incluso dañar la integridad de las personas, es el caso de los Virus informáticos, sabotajes estafas, robo, etc.
- **Amenazas de agentes internos:** son eventos producidos por los mismos empleados que forman parte de la empresa, debido al

desconocimiento en el manejo de las herramientas de seguridad y protección de datos.

Adicionalmente las Amenazas se clasifican según el grado de intencionalidad:

- **Accidentes:** son acontecimientos imprevistos que interfieren en el resguardo de la información por ejemplo averías del hardware, incendio, etc.
- **Errores:** está fuertemente condicionado por el desempeño de las personas en el manejo del software o hardware.
- **Actuaciones malintencionadas:** las personas buscan obtener dinero o simplemente por afectar a la integridad de los demás tal es el caso de los robos, fraudes, sabotajes etc.

b. Vulnerabilidades

Según Gómez, A. (2011) “una vulnerabilidad es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.”

Así también se encuentra vulnerabilidades desde los siguientes puntos de vista:

- **Vulnerabilidades de software:** se da ciertos errores en las aplicaciones o sistemas operativos.
- **Vulnerabilidades de hardware:** Por su inadecuada seguridad física o incluso mal manejo del equipo informático.
- **Vulnerabilidades de datos:** inadecuados controles de acceso a personal no autorizado
- **Vulnerabilidades administrativas:** principalmente ocasionado por la ausencia de políticas, cultura y capacitación en temas de seguridad para proteger la información.
- **Vulnerabilidades de comunicaciones:** inadecuados controles de acceso a la red.

- **Vulnerabilidades de personal (empleados):** inadecuados controles de acceso físico.

c. Incidentes de seguridad

Según Guzmán, A. (2011) “un Incidente de Seguridad Informática está definido como un evento que atenta contra la Confidencialidad, Integridad y Disponibilidad de la información y de los recursos tecnológicos.”

En definitiva un incidente de seguridad compromete a la efectividad de las operaciones del negocio y atenta contra la protección de la información, además un incidente causa impacto sobre cualquiera de las dimensiones de seguridad, puede ocurrir de que la información no está accesible por los usuarios autorizados, o incluso un usuario no autorizado ha tenido acceso a la información y que pudo haberla modificado.

d. Impactos.

El impacto es la medición y valoración del daño que podría producir a la organización un incidente de seguridad. Gómez, A. (2011)

En definitiva el impacto son las consecuencias de no aplicar herramientas y demás medidas de seguridad que permitan proteger la información de las empresas.

e. Defensas, salvaguardias o medidas de seguridad

Si bien es cierto, las amenazas están íntimamente ligadas con las vulnerabilidades del sistema informático, al establecer medidas o controles de seguridad se intenta reducir los riesgos de ataques cibernéticos que afectan económicamente a las empresas.

2.2.9. Presupuesto- Inversión en Seguridad de la Información

a. Inversión

De acuerdo a BBVA (2017) inversión se refiere al “acto de postergar el beneficio inmediato del bien invertido por la promesa de un beneficio futuro más o menos probable” (p.1).

b. Presupuesto de inversiones

Como señala en el Blog Clase & Calidad (2013) el presupuesto de inversiones “representa todo aquello en donde la empresa debe Invertir para un propósito que va más allá del ejercicio económico de un año”

En torno al tema de inversión en seguridad de la información hay que considerar varios aspectos, la inversión que cada entidad deba realizar va a depender del valor que represente el activo (información) para el funcionamiento de la empresa. Actualmente el panorama de seguridad muestra a las organizaciones que deben realizar un presupuesto en este sentido ya que son varias las consecuencias que podría producir la ciberdelincuencia.

Al momento de identificar el presupuesto es importante que estas inversiones en seguridad estén alineadas con los riesgos identificados que podrían afectarlos, además de tener bien identificados cuales son los activos de información importantes para la entidad, según la página web Computing (2016) menciona que el gasto real en seguridad está “dividido entre hardware, software, servicios (outsourcing y consultoría) y personal”, pero referente a la verdadera magnitud de inversión se considera “características de seguridad que se incorporan en hardware, software, u otras actividades iniciativas no específicamente dedicadas a la seguridad”.

Así también en base al informe de Gartner publicado en la página web Computing (2016) menciona que las empresas no tienen bien definido o simplemente no conocen cuál es su presupuesto en seguridad, a veces ni la persona encargada en el tema de seguridad de TI en la empresa no tiene información sobre la inversión en seguridad de toda la organización, esto se debe según Gartner en parte al hecho de que “pocos sistemas de contabilidad desglosan la seguridad como una línea de pedido separada y muchos procesos relacionados con la seguridad son llevados a cabo por personal que no está dedicado a tiempo completo a la seguridad.”

Para desarrollar un adecuado presupuesto de inversión en temas de seguridad de la información se debe basar en los conocimientos de un

Oficial de Seguridad de la Información (CISO) de la empresa ya que él es quien conoce a fondo las necesidades a implementar para la protección de los sistemas de información.

2.2.10. Beneficio - Retorno de Inversión en Seguridad (ROSI)

Este es un indicador que nos permite determinar si una inversión en seguridad es rentable desde el punto de vista financiero de modo que los costos en seguridad sean menor que el activo que se protege.

Hay que considerar que las inversiones en seguridad de la información no representan un retorno directo de ingresos de dinero por su implementación, por lo tanto estas inversiones no son realizadas con el fin de generar ingresos para la entidad, pero a través del ROSI se puede analizar los beneficios económicos que están relacionados a las inversiones en seguridad, en este sentido podemos hacer referencia a un enfoque en un panorama de posibles riesgos y amenazas a los que se enfrentan las empresas en donde aquellas medidas de seguridad adaptadas prevendrán estos acontecimientos y de esa forma se evitara el impacto económico en la entidad.

El sentido que se da al Retorno de Inversión en Seguridad es que este indicador “permite evaluar cuánto dinero se dejará de perder” (Bortnick, 2010).

Fórmula para el cálculo del ROSI

$\text{ROSI} = (\text{Disminución del riesgo} - \text{Costos de inversión}) / \text{Costos de inversión}$
$\text{ROSI} = [(\text{Riesgo de exposición} * \% \text{ Riesgo mitigado}) - \text{Costos de inversión}] / \text{Costos de inversión}$
$\text{Riesgo de exposición} = \text{Coste de un incidente} * \text{Tasa de ocurrencia anual}$

Figura 2. Fórmula para el cálculo del ROSI

2.2.11. Organismos de Control

a. Superintendencia de Compañías

Según el portal de la Superintendencia de Compañías (2018) indica que este es “un organismo técnico, con autonomía administrativa y económica,

que vigila y controla la organización, actividades, funcionamiento, disolución y liquidación de las compañías y otras entidades en las circunstancias y condiciones establecidas por la Ley”.

La Superintendencia de Compañías Valores y Seguros a través de su portal de información nos da a conocer la Clasificación Industrial Internacional Uniforme (CIIU) el cual abarca una estructura de clasificación de todas las actividades económicas que realizan las empresas dentro de un sector de la economía. Para la investigación se trabajara con un grupo seleccionado de empresas pertenecientes al ramo de enseñanza, salud, alojamiento y ramo administrativo y de apoyo.

b. Superintendencia de Economía Popular y Solidaria (SEPS)

Según el portal web de la SEPS (2018) manifiesta que es una “entidad técnica de supervisión y control de las organizaciones de la economía popular y solidaria, con personalidad jurídica de derecho público y autonomía administrativa y financiera, que busca el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario”.

- **Sector financiero**

Para la investigación se ha considerado el sector cooperativo regulado por este organismo, que viene hacer un conjunto de cooperativas como sociedades de personas cuya actividad y relaciones, se sujetarán a los principios establecidos en la Ley Orgánica de Economía Popular y Solidaria y del Sector Financiero Popular y Solidario, a los valores y principios universales del cooperativismo y a las prácticas de Buen Gobierno Corporativo.

Las entidades del sector Financiero Popular y Solidario se ubican de acuerdo a la segmentación que determine la Junta de Política y Regulación Monetaria y Financiera, por lo tanto considerando el tipo y el saldo de sus activos se ubicarán en los siguientes segmentos:

Tabla 1**Segmentación de entidades del SFPS**

Segmento	Activos (USD)
1	Mayor a 80'000.000,00
2	Mayor a 20'000.000,00 hasta 80'000.000,00
3	Mayor a 5'000.000,00 hasta 20'000.000,00
4	Mayor a 1'000.000,00 hasta 5'000.000,00
5	Hasta 1'000.000,00 Cajas de Ahorro, bancos comunales y cajas comunales

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

El monto para cada uno de los segmentos será actualizado anualmente por la Junta aplicando la variación del índice de precios al consumidor.

2.3. Base Legal

2.3.1. Constitución de la República del Ecuador

En base a la Constitución de la República del Ecuador (2008) registro oficial No 449 de 20-oct-2008, según el Art 66, numeral 3: “El derecho a la integridad personal, que incluye la integridad física, psíquica, moral y sexual”

Constitución de la República del Ecuador (2008), registro oficial No 449 de 20-oct-2008, según el Art 66, numeral 19:

El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Constitución de la República del Ecuador (2008), registro oficial No 449 de 20-oct-2008, según el Art 66, numeral 20: “El derecho a la intimidad personal y familiar”

2.3.2. Plan Nacional del Buen Vivir

Secretaría Nacional de Planificación y Desarrollo (2013), objetivo 6 del Plan Nacional del Buen Vivir: “Consolidar la transformación de la justicia y fortalecer la seguridad integral, en estricto respeto a los derechos humanos”.

En este objetivo el gobierno ecuatoriano lo que busca es fomentar la justicia, este principio moral se lleva a cabo respetando siempre la verdad, y otorgando repesarías para quien sea merecido, por tanto como consecuencia del cumplimiento efectivo de este punto hace posible la seguridad integral de la sociedad.

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

Proyecto de Ley Organica de la Proteccion de los Derechos a la Intimidad y Privacidad sobre los Datos Personales (2016), según el Art. 1:

Objeto.- La presente Ley tiene por objeto proteger y garantizar el derecho de todas las personas a la intimidad y privacidad en el tratamiento de datos personales que se encuentran en bases o banco de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas.

2.3.4. Ley Orgánica de Transparencia y Acceso a la Información Pública

Ley Orgánica de Transparencia y Acceso a la Información Pública (2004) registro oficial No 337 de 18-may-2004, según el Art 2, literal d: “Garantizar la protección de la información personal en poder del sector público y/o privado”

2.3.5. Ley del Sistema Nacional de Registros de Datos Públicos

Ley del Sistema Nacional de Registros de Datos Públicos (2012), según el Art. 4:

Responsabilidad de la información.- Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo.

Ley del Sistema Nacional de Registros de Datos Públicos (2012), según el Art. 6:

Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

2.3.6. Ley Orgánica de la Gestión de la Identidad y Datos Civiles

La Ley Orgánica de la Gestión de la Identidad y Datos Civiles (2016), registro oficial 684, Art. 3 objetivos, Inciso 4, 5,6:

- Proteger la confidencialidad de la información personal.
- Evitar el sub-registro o carencia de datos en registro de una persona.
- Proteger la información almacenada en archivos y bases de datos de los hechos y actos relativos al estado civil de las personas.

2.3.7. Código Orgánico Integral Penal

Código Orgánico Integral Penal (2014), sección Sexta, Delitos Contra la Intimidad Personal, Art 178:

Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

2.4. Sistemas de variables

2.4.1. Variable dependiente

Costo-Beneficio para las empresas del sector servicios reguladas por la Superintendencia de Compañías y por la SEPS en sistemas de protección de datos.

2.4.2. Variable independiente

Inversión en la aplicación de herramientas de seguridad de la información

2.5. Hipótesis

2.5.1. 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.

2.5.2. 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.

2.6. Operacionalización de variables

Tabla 2

Cuadro de Operacionalización de variables

OBJETIVO GENERAL: Analizar el costo – beneficio de invertir en herramientas de seguridad y protección de datos de las empresas del sector servicios reguladas por la Superintendencia de Compañías y la SEPS de la Provincia de Cotopaxi durante el periodo 2012-2016, para proponer un simulador que permita el retorno de la inversión de la seguridad de la información.				
Objetivos Específicos	Variables	Dimensión	Indicador	Instrumentos
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.	Costo-beneficio y seguridad de la información	Bases Teóricas	Documental	Fuentes de información primaria y secundaria
Identificar las características y porcentajes de inversión en seguridad informática de las empresas del	Herramientas de Seguridad y protección de datos	Superintendencia de Compañías y la SEPS	Porcentaje de inversión en herramienta s de S.I.	Estados Financieros

sector servicios reguladas por la Superintendencia de Compañías y la SEPS para un correcto desarrollo del trabajo investigativo.

Determinar en base a la 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.	Herramientas de Seguridad y protección de datos	Controles de ISO/IEC 27002	Gestión de los sistemas de información	Encuesta
--	---	----------------------------	--	----------

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.	Costo-beneficio/ Herramientas de S.I:	Simulador	Nº y costo de los incidentes	Análisis de los problemas en S.I
--	--	-----------	------------------------------	----------------------------------

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Enfoque de la investigación

Para Hernández, Fernández, & Baptista (2010) en su libro Metodología de la investigación indica que el enfoque cuantitativo “Utiliza la recolección de datos para probar hipótesis, previamente hechas, con base en la medición numérica, el conteo y frecuentemente en el uso de estadística para establecer patrones de comportamiento en una población” (p.46).

Para Hernández, Fernández, & Baptista (2010) en su libro Metodología de la investigación indica que el enfoque cualitativo “utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación” (p.49)

En tal sentido la investigación abarca un enfoque cuantitativo, debido a que se fundamenta de pruebas numéricas y estadísticas para comprobar la hipótesis de la investigación. Así también se utiliza el enfoque cualitativo debido a que, se aplica técnicas e instrumentos de recolección de datos como es la encuesta, cuyos resultados nos permiten la interpretación y el análisis de la situación actual en cuanto a la gestión de herramientas para la protección de datos en las empresas.

3.2. Modalidad de la investigación

3.2.1. Bibliográfica – documental

De acuerdo a Rodríguez M. (2013) en su plataforma virtual define a la investigación bibliográfica documental como:

Una parte esencial de un proceso sistemático de investigación científica, constituyéndose en una estrategia operacional donde se observa y reflexiona sistemáticamente sobre realidades (teóricas o no) usando para ello diferentes tipos de documentos. La ID Indaga, interpreta, presenta datos e informaciones sobre un tema determinado de cualquier ciencia, utilizando para ello, una metódica de análisis y teniendo como finalidad obtener resultados que pudiesen ser base para el desarrollo de una investigación científica.

La investigación documental forma parte de la investigación ya que se requirieron distintas fuentes de consulta para recolectar información que permitió realizar el marco teórico, conceptual, legal y demás puntos a desarrollar para lo cual se acudió a distintas fuentes bibliográficas como libros, revistas, y demás documentos que ayuden a sustentar el tema objeto de estudio y a través de esa información poder emitir criterios coherentes a los resultados.

3.2.2. De campo

Según Arias F. (2012) en su texto define lo siguiente con respecto a la investigación de campo:

Es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), *sin manipular o controlar variable alguna*, es decir, el investigador obtiene la información pero no altera las condiciones existentes (p.31)

Este enfoque de investigación lo llevaremos a cabo en el proyecto ya que la información a considerar para comprobar la hipótesis del caso de investigación partirá de obtener datos directamente de la fuente objeto de estudio, utilizando técnicas de recolección de información como son la observación directa en el lugar, y la aplicación de encuestas lo cual dará más relevancia a los datos obtenidos en la investigación.

3.3. Nivel o tipo de investigación

3.3.1. Investigación exploratoria

De acuerdo a los autores Hernández, Fernández, & Baptista (2010) en su texto Metodología de la Investigación define a la investigación exploratoria como:

Estudios que se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde nuevas perspectivas (p. 79)

Considerando lo expuesto anteriormente, para la investigación se aplicara el método exploratorio ya que se aborda un contexto particular donde existe poca información acerca del tema de investigación, por lo tanto a través de este estudio se realiza una primera habladuría y acercamiento de que está sucediendo en las empresas del sector servicios reguladas por los respectivos organismos de control de la provincia de Cotopaxi en razón a la inversión en herramientas de seguridad y protección de datos, de este modo se aportará ciertas bases y una temática donde se pueda sustentar las investigaciones posteriores en este ámbito.

3.3.2. Investigación descriptiva

El autor Arias F. (2012) en su libro El Proyecto de Investigación nos dice:

La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere. (p.24)

La investigación descriptiva en la presente investigación será de utilidad debido a que permitirá describir de modo sistemático características de forma autónoma e independiente del área de interés a investigar, además medir las variables de estudio.

3.4. Población y Muestra

3.4.1. Población

Según Marradi, Archenti, & Piovani, (2007) en su texto define a la población como: “Conjunto de ejemplares de esa unidad que se encuentran en un ámbito espacio-temporal.” (p.88)

Con la definición anteriormente expuesta, se atribuye que la población objeto de este trabajo investigativo está constituido por 548 empresas de Servicios reguladas por la Superintendencia de Compañías y más 62 cooperativas de ahorro y crédito de los segmentos uno, dos, tres, cuatro y cinco reguladas por la Superintendencia de Economía Popular y Solidaria,

representando un total 610 entidades de servicios como unidad de análisis, mismas que están ubicadas en la Provincia de Cotopaxi.

3.4.2. Muestra

Según Marradi, Archenti, & Piovani, (2007) en su texto define a la muestra como: “Cualquier subconjunto amplísimo o limitadísimo de miembros de una población que se investiga. Su fin es extender a toda la población las conclusiones resultantes del análisis de las informaciones relativas al subconjunto.” (p.89)

Para el desarrollo de esta investigación se procede a determinar de forma más específica las empresas a analizar, que estén bajo las condiciones requeridas para el estudio, enfocados en dicho fin se aplicará un tipo de muestreo intencional y al azar simple para lo cual el autor Arias (2012) menciona que muestreo intencional consiste en que “los elementos son escogidos con base en criterios o juicios preestablecidos por el investigador” (p. 85), de igual manera Arias (2012) con respecto al muestreo al azar simple indica que es el “procedimiento en el cual todos los elementos tienen la misma probabilidad de ser seleccionados” (p. 84).

Por las razones anteriormente citadas se desagrega la muestra sobre la base de la población existente, en forma porcentual considerando a las entidades reguladas por los respectivos organismos de control, que en sus balances de los años 2012 al 2016, dentro de este periodo se refleje o exista un nivel de crecimiento de los valores correspondientes a las cuentas equipo de cómputo y software.

En tal sentido para el análisis y la aplicación de encuestas se escogió a cuatro empresas reguladas por la Superintendencia de Compañías cada una perteneciente a distintos ramos de actividad económica, así mismo se escogió a 22 cooperativas de ahorro y crédito de los segmentos uno, dos, tres y cuatro. Por sigilo de su denominación se las conocerá como casos de estudio. En la siguiente tabla se muestran los casos de investigación a analizar mediante el muestreo intencional sobre el costo- beneficio de invertir en herramientas de seguridad y protección de datos:

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

Tabla 4**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

3.1. Fuentes de información

Ruíz, M. y Vargas, J. (2008) en su artículo sobre Fuentes de información establece:

Son todos los recursos que contienen datos formales, informales, escritos, orales o multimedia. Se dividen en tres tipos: primarias, secundarias y terciarias.

Fuentes primarias: Contienen información original, que ha sido publicada por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más.

Fuentes secundarias: Contienen información primaria, sintetizada y reorganizada.

Fuentes terciarias: Son guías físicas o virtuales que contienen información sobre las fuentes secundarias.

Para el presente trabajo, las fuentes de información, constituyen el pilar fundamental para iniciar con la investigación, en este caso se utilizará fuentes primarias y secundarias de información, estos a su vez contienen datos útiles para generar el conocimiento.

3.5. Técnicas de recopilación de información

3.5.1. Instrumentos de la investigación

Moreno, E. (2013) En su investigación sobre los Instrumentos de Investigación establece que: “Es la herramienta utilizada por el investigador para recolectar la información de la muestra seleccionada y poder resolver el problema de la investigación.”

Gonzalez, W. (2009) en su artículo publicado denominado Recolección de datos enfatiza:

Los analistas utilizan una variedad de métodos a fin de recopilar los datos sobre una situación existente, como entrevistas, encuestas, inspección de registros (revisión en el sitio) y observación. Cada uno tiene ventajas y desventajas. Generalmente, se utilizan dos o tres para complementar el trabajo de cada una y ayudar a asegurar una investigación completa.

Para obtener información acerca del tema de estudio y así poder comprobar la hipótesis de la investigación se aplicará encuestas dirigidas para los gerentes y miembros del departamento de tecnología de las empresas de servicios reguladas por la Superintendencia de Compañías y la SEPS, permitiendo recopilar información para obtener datos congruentes en relación con el tema de estudio, y lograr dar una opinión crítica sobre la situación planteada.

3.5.2. Definición de los sujetos/unidades de información

Las personas que intervendrán en la investigación de forma directa son el gerente, y miembros de las áreas de tecnología de las empresas de servicios reguladas por la Superintendencia de Compañías y la SEPS, se constituyen como unidad u objeto de análisis de la presente investigación.

3.5.3. Validación y confiabilidad

Validez

Según Corral (2009), indica que:

La validez responde a la pregunta ¿con qué fidelidad corresponde el universo o población al atributo que se va a medir?. La validez de un instrumento consiste en que mida lo que tiene que medir (autenticidad), algunos procedimientos a emplear son: Know groups (preguntar a grupos conocidos) (p. 230)

Confiabilidad

Según Corral (2009), indica que:

La confiabilidad responde a la pregunta ¿con cuánta exactitud los ítems, reactivos o tareas representan al universo de donde fueron seleccionados? El término confiabilidad designa la exactitud con que un conjunto de puntajes de pruebas miden lo que tendrían que medir (p.239)

Para la investigación se procederá a la validación de la encuesta que se utilizará en el estudio sobre el “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”.

3.6. Técnicas de análisis de datos

Para el análisis de los datos obtenidos a través de la encuesta se ha considerado hacer uso de la herramienta estadística SPSS y Microsoft Excel, mismos que ayudarán a obtener información oportuna y detallada que sirvan de base para comprobar la hipótesis planteada y dar cumplimiento a los objetivos específicos expuestos en la presente investigación.

3.7. Técnicas de comprobación de hipótesis

Para comprobar la hipótesis, se utilizó la prueba del Chi-cuadrado siendo una “prueba de hipótesis que compara la distribución observada de los datos con una distribución esperada de los datos”, por lo que permite establecer si existe o no relación entre las variables de la presente investigación.

CAPÍTULO IV

4. RESULTADOS DE LA INVESTIGACIÓN

En el presente capítulo se procederá analizar por grupo de empresas la estructura organizativa con el fin de identificar la información que se maneja en cada uno de los departamentos, seguidamente se consideró el crecimiento dentro del periodo estudiado en la cuenta equipo de cómputo. Así también se da a conocer los resultados obtenidos de las encuestas aplicadas a las empresas del sector servicios Reguladas por la Superintendencia de compañías correspondientes a los ramos de enseñanza, salud, alojamiento, actividades administrativas y de apoyo, adicionalmente se encuestó a las entidades Reguladas por la SEPS de los segmentos uno, dos, tres y cuatro, la aplicación de este instrumento nos permitió recolectar información que nos servirá de base para comprobar la hipótesis.

Para dar cumplimiento al segundo objetivo “Identificar las características y porcentajes de inversión en seguridad informática de las empresas del sector servicios, se procede a realizar el análisis de la estructura organizativa y el crecimiento del equipo de cómputo:

4.1. Análisis de la estructura organizativa de las empresas.

Por motivo de la complejidad que conlleva el análisis de inversiones en herramientas de seguridad y protección de datos por cada empresa que forma parte de los doce segmentos correspondientes al sector servicios reguladas por los organismos de control SC Y la SEPS, y en base a los antecedentes recopilados de la presente investigación se determinó que los incidentes de seguridad en la información predominan en los segmento de actividades de alojamiento y de servicios de comidas, enseñanza, actividades de atención de la salud humana y de asistencia social, actividades de servicios administrativos y de apoyo, y actividades financieras.

Por el número de empresas que abarca la investigación se considera apropiado identificar los departamentos más comunes que manejen

información propensa a ataques informáticos y fugas de información, esto facilitará la asignación de controles considerando el tipo de información que maneje el departamento.

Tabla 5

Estructura organizacional entidades de alojamiento

DEPARTAMENTO / ÁREA	SUB-DEPARTAMENTOS	DESCRIPCIÓN	ACTIVIDADES/ TIPO DE INFORMACIÓN QUE MANEJAN
Financiera	Contabilidad	Maneja y lleva un control de las operaciones financieras que ocurren en la empresa	<ul style="list-style-type: none"> • Información financiera
	Tesorería	Se encarga de pagos de nómina y proveedores del lugar	<ul style="list-style-type: none"> • Registro de proveedores • Relación con entidades financieras y bancarias
Administrativa	Talento Humano	Responsables de la organización del personal, selección previa, coordinación y mantenimiento del personal	<ul style="list-style-type: none"> • Nómina • Contratos laborales • Programas de capacitación y entrenamiento de empleados
	Mercadeo y Publicidad	Se encarga de las ventas y publicidad ,	<ul style="list-style-type: none"> • Estrategias de publicidad y promoción
Recepción	Recepción	Se encarga de recibir al huésped y orientarlos durante su estancia	<ul style="list-style-type: none"> • Asignación de habitaciones y reservaciones • Registros de entrada y salida del huésped • Confirmar y cancelar reservaciones

CONTINÚA 

	Guardia de seguridad	Seguridad física durante las 24 horas a los huéspedes y demás instalaciones	<ul style="list-style-type: none"> • Patrullan a pie por dentro y fuera de la empresa, observando comportamientos sospechosos y principales amenazas.
Alojamiento	Camareros	Brinda atención a los comensales y mantienen limpia el área.	<ul style="list-style-type: none"> • Toma nota de los pedidos comidas o bebidas • Preparar la cuenta y cobra el consumo en la mesa
	Auxiliares de Habitaciones	Se encarga del orden, la higiene y aseo las habitaciones y de los implementos de las mismas.	<ul style="list-style-type: none"> • Reporta necesidades de mantenimiento, objetos olvidados. • Atiende al cliente durante su permanencia
Bodega	Bodega	Gestionar el abastecimiento de las materias primas, alimentos y bebidas destinadas a la cocina	<ul style="list-style-type: none"> • Registro de inventarios
Mantenimiento	Habitaciones	Precautelar el óptimo funcionamiento de las instalaciones del hotel	<ul style="list-style-type: none"> • Acceso a las habitaciones

Tabla 6

Estructura organizacional entidades de enseñanza

DEPARTAMENTO / ÁREA	SUB-DEPARTAMENTOS	DESCRIPCIÓN	ACTIVIDADES/ TIPO DE INFORMACIÓN QUE MANEJAN
Contabilidad	Contabilidad	Lleva acabo asuntos contables y financieros proporcionando información económica oportuna.	<ul style="list-style-type: none"> • Información financiera
Secretaria / Colecturía	Secretaria / Colecturía	Recaudar los ingresos propios del establecimiento	<ul style="list-style-type: none"> • Registros de recaudaciones por pensiones • Manejo de la documentación y archivo de la institución • Datos personales y académico de los estudiantes
Dirección académica	Dirección académica	Gestiona el funcionamiento académico de la institución mediante servicios de evaluación, asesoría y control	<ul style="list-style-type: none"> • Políticas y regulaciones • Programas académicos y curriculares • Evaluaciones y seguimientos académicos a docentes
Colectivo Talento humano	Colectivo Talento humano	Gestiona el talento humano de la organización en beneficio absoluto del individuo y de la propia empresa.	<ul style="list-style-type: none"> • Planificación, selección y formación de personal. • Datos personales de los docentes
Inspección General	Sub-Inspección General	Velar por el cumplimiento de las normas y disposiciones institucionales	<ul style="list-style-type: none"> • Registros disciplinarios • Registros de asistencia
Estudiantes	Estudiantes	Participar activamente en el proceso de enseñanza y aprendizaje	<ul style="list-style-type: none"> • Acoger las disposiciones reglamentarias

Tabla 7

Estructura organizacional entidades de salud

DEPARTAMENTO / ÁREA	SUB-DEPARTAMENTOS	DESCRIPCIÓN	ACTIVIDADES/ TIPO DE INFORMACIÓN QUE MANEJAN
Administrativa	Contabilidad	Maneja y lleva un control de las operaciones contables y financieras de la institución	<ul style="list-style-type: none"> • Cobros y facturas a pacientes • Control de gastos. • Informe económico o los cuadros de caja.
Servicios médicos	Quirófanos	El Quirófano es un área dentro del Hospital donde se opera a los pacientes	<ul style="list-style-type: none"> • Información técnica sobre los instrumentos del quirófano • Información del paciente: Historial clínico. • Datos personales
Servicios Auxiliares, Diagnóstico y Tratamiento	Laboratorio	En el laboratorio clínico se obtienen y se estudian muestras biológicas diversas, como sangre, orina y heces	<ul style="list-style-type: none"> • Exámenes médicos
Servicios Técnicos de Colaboración Medica	Farmacia	Distribución y gestión de los medicamentos.	<ul style="list-style-type: none"> • Inventario de medicamentos
Servicios generales	Vigilancia	Vigilancia y protección del edificio	<ul style="list-style-type: none"> • Control de entradas y salidas extraordinarias de visitantes
	Mantenimiento	Lograr el mantenimiento preventivo y correctivo de la infraestructura, mobiliario, equipos, ambulancias y otros vehículos del Hospital.	<ul style="list-style-type: none"> • Registros de acceso a las instalaciones
	Limpieza	Lograr que se mantenga asepsia e higiene en especial en las áreas críticas.	

Tabla 8

Estructura organizacional entidades de Administración y de Apoyo

DEPARTAMENTO / ÁREA	SUB-DEPARTAMENTOS	DESCRIPCIÓN	ACTIVIDADES/ TIPO DE INFORMACIÓN QUE MANEJAN
Ventas	Counter	Se encarga de proyectar la imagen de la empresa y desarrollar las técnicas de procedimiento de atención y recepción al cliente.	<ul style="list-style-type: none"> • Registro de los usuarios en el sistema • Información de proveedores de productos turísticos. • Recepción de los cobros por ventas
Contabilidad	Contabilidad	Maneja y lleva un control de las operaciones contables y financieras de la institución	<ul style="list-style-type: none"> • Recibe y clasifica todos los documentos que le sean asignado • Prepara los estados financieros y balances de ganancias • Emite cheques correspondientes a pagos de proveedores y servicios de personal.
Mensajero	Mensajero	Es el responsable de llevar mercancías, bultos o paquetes de un lugar a otro.	<ul style="list-style-type: none"> • Entrega de la documentación administrativa oportuna, con el cumplimiento de los datos del que entrega y del que recibe, con las firmas oportunas y los horarios de entrega-recogida. • Entrega de documentos para clientes de la Compañía

Tabla 9

Estructura organizacional Cooperativas de Ahorro y Crédito

DEPARTAMENTO / ÁREA	SUB-DEPARTAMENTOS	DESCRIPCIÓN	ACTIVIDADES/ TIPO DE INFORMACIÓN QUE MANEJAN
Negocios	Crédito y cobranzas	Evalúa el riesgo de financiar temporalmente a sus clientes y por otra parte procurar el pago oportuno del crédito.	<ul style="list-style-type: none"> • Condición económica de los socios • Prestamos vinculados. • Situación financiera de la Cooperativa • Morosidad de los socios • Políticas y estrategias de crédito y cobranzas
	Captaciones	Captar recursos de socios /clientes en depósitos de ahorros en sus diferentes modalidades.	<ul style="list-style-type: none"> • Sigilo bancario respecto de la información de los socios/clientes así como de sus movimientos transaccionales • Información pólizas de deposito • Custodiar documentos de los depósitos a plazo fijo, debidamente clasificados y ordenados y mantener dichos documentos en un lugar seguro
Talento Humano	Talento Humano	Administrar la gestión del talento humano en la institución y buscar la conjugación del desarrollo profesional de los colaboradores con los objetivos institucionales.	<ul style="list-style-type: none"> • Información personal de los empleados (fichero de los empleados) como sueldo, desempeños profesionales o bajas laborales
Contabilidad	Contabilidad	Registra y procesa las transacciones económicas de la Cooperativa	<ul style="list-style-type: none"> • Información financiera de la cooperativa

CONTINÚA 

Financiero	Financiero	Mantiene relaciones de coordinación con la Gerencia General, los encargados de los demás departamentos y el responsable del sistema de información, controlando el área financiera, contable y administrativa de la Cooperativa	<ul style="list-style-type: none"> • Información financiera de la Cooperativa • Información personal y económica de socios • Deudores morosos
Tesorería	Tesorería	Gestionar las operaciones de flujos monetarios, como es la ejecución de pagos y cobros, la gestión de la caja y las diversas gestiones bancarias. Encargarse de la liquidez necesaria de la cooperativa.	<ul style="list-style-type: none"> • Información financiera de la Cooperativa
Operaciones	Mantenimiento y Sistemas	Identifica los requerimientos de automatización de la entidad, y el cumplimiento de estructuras para los Organismos de Control, recomienda su adquisición y mantiene operativos y seguros, los equipos y programas.	<ul style="list-style-type: none"> • Información financiera de la Cooperativa • Información personal de los socios y deudores
	Cajas	Captación, entrega y custodia de dinero en efectivo, cheques, giros y demás documentos de valor, logrando la recaudación de ingresos a la institución y la cancelación de pagos que correspondan a través de caja	<ul style="list-style-type: none"> • Responsable directo del dinero en efectivo, cheques y otros documentos de valor.
	Servicio al cliente	Atención personalizada, ágil, eficaz al socio sobre los distintos productos y servicios que ofrece la cooperativa y proporcionara la información de créditos vencidos y preparara las notificaciones para los socios morosos.	<ul style="list-style-type: none"> • Datos personales de clientes y socios de la Cooperativa • Información económica de los socios deudores

4.2. Análisis del crecimiento en equipo de cómputo

Entidades reguladas por la SEPS

Tabla 10

Crecimiento equipo de cómputo - Segmento 1

	Año 2012	Año 2013	Año 2014	Año 2015	Año 2016
Caso 1	\$ 712.961,97	\$ 873.331,25	\$ 955.776,76	\$ 1.032.230,38	\$ 1.234.952,88
% Crecimiento		22,49%	9,44%	8,00%	19,64%

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

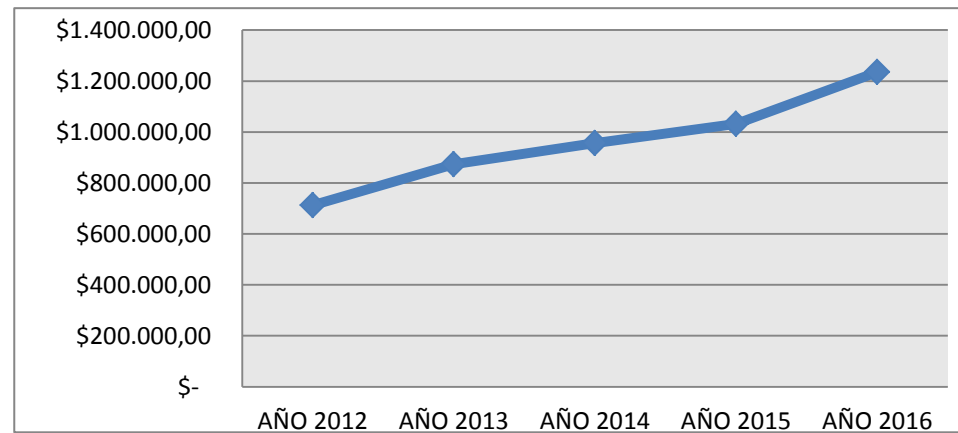


Figura 3. Crecimiento equipo de cómputo – Segmento 1

La entidad del segmento financiero uno durante el periodo 2012-2016 tuvo un crecimiento porcentual promedio de 14,89% en la cuenta equipo de cómputo.

Tabla 11

Crecimiento equipo de cómputo - Segmento 2

	Año 2012	Año 2013	Año 2014	Año 2015	Año 2016
Caso de estudio 2	\$ 35.282,95	\$ 35.282,95	\$ 58.754,26	\$ 58.480,31	\$ 90.519,69
Caso de estudio 3	\$ 92.621,38	\$ 79.247,81	\$ 89.405,79	\$ 115.088,59	\$ 128.334,16
Promedio	\$ 63.952,17	\$ 57.265,38	\$ 74.080,03	\$ 86.784,45	\$ 109.426,93
% de Crecimiento		-10,46%	29,36%	17,15%	26,09%

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

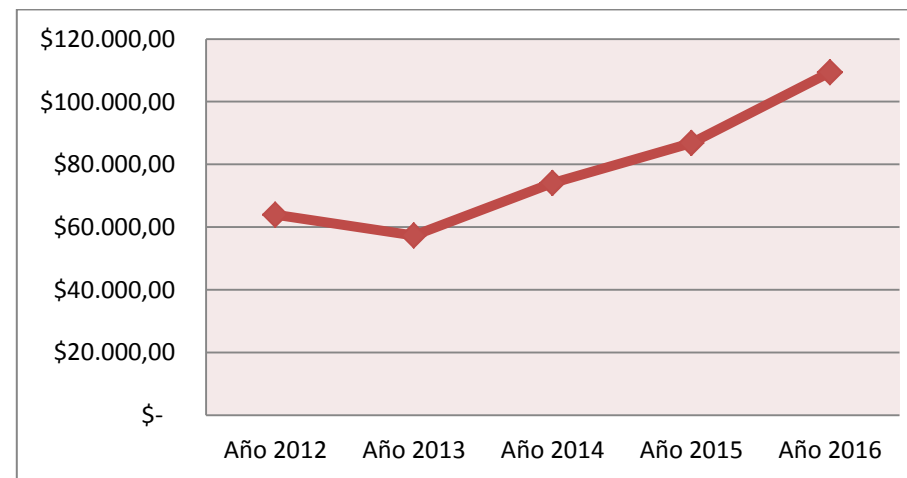


Figura 4. Crecimiento equipo de cómputo – Segmento 2

Las 2 entidades del segmento financiero dos durante el periodo 2012-2016 tuvieron un crecimiento porcentual promedio de 15,54% en la cuenta equipo de cómputo.

Tabla 12

Crecimiento equipo de cómputo - Segmento 3

	Año 2012	Año 2013	Año 2014	Año 2015	Año 2016
Caso de estudio 4	\$ 39.544,05	\$ 39.544,05	\$ 75.530,24	\$ 90.913,86	\$ 111.877,61
Caso de estudio 5	\$ 33.715,83	\$ 33.715,83	\$ 45.114,78	\$ 56.289,57	\$ 66.002,49
Caso de estudio 6	\$ 56.912,82	\$ 56.912,82	\$ 70.894,46	\$ 82.373,48	\$ 106.052,52
Caso de estudio 7	\$ 116.793,15	\$ 116.793,15	\$ 125.579,15	\$ 131.863,72	\$ 138.358,50
Caso de estudio 8	\$ 32.851,17	\$ 32.851,17	\$ 66.458,18	\$ 92.695,26	\$ 111.638,68
Promedio	\$ 55.963,40	\$ 55.963,40	\$ 76.715,36	\$ 90.827,18	\$ 106.785,96
% de Crecimiento		0,00%	37,08%	18,40%	17,57%

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

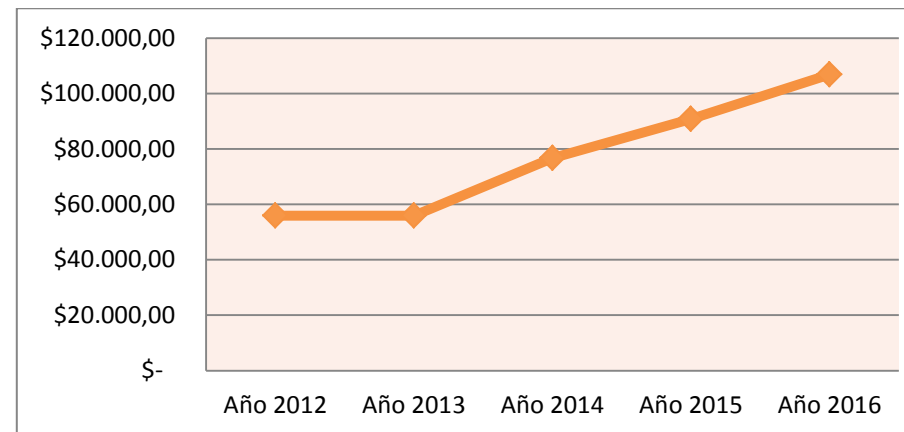


Figura 5 Crecimiento equipo de cómputo – Segmento 3

Las 5 entidades del segmento financiero tres durante el periodo 2012-2016 tuvieron un crecimiento porcentual promedio de 18,26% en la cuenta equipo de cómputo.

Tabla 13

Crecimiento equipo de cómputo - Segmento 4

	Año 2012	Año 2013	Año 2014	Año 2015	Año 2016
Caso de estudio 9	\$ 14.166,32	\$ 14.166,32	\$ 16.864,92	\$ 17.812,71	\$ 17.117,04
Caso de estudio 10	\$ 20.556,15	\$ 20.556,15	\$ 28.270,84	\$ 29.781,72	\$ 29.781,72
Caso de estudio 11	\$ 14.740,36	\$ 14.740,36	\$ 19.216,70	\$ 16.374,70	\$ 16.754,70
Caso de estudio 12	\$ 6.609,28	\$ 6.609,28	\$ 4.674,63	\$ 10.400,28	\$ 11.143,28
Caso de estudio 13	\$ 17.435,69	\$ 17.435,69	\$ 26.207,52	\$ 26.738,77	\$ 30.104,16
Caso de estudio 14	\$ 8.955,86	\$ 8.955,86	\$ 8.955,86	\$ 9.939,93	\$ 11.560,43
Caso de estudio 15	\$ 18.513,18	\$ 18.513,18	\$ 19.985,03	\$ 19.985,03	\$ 22.515,46
Caso de estudio 16	\$ 5.720,90	\$ 5.720,90	\$ 7.952,90	\$ 9.083,30	\$ 11.283,90
Caso de estudio 17	\$ 9.098,08	\$ 9.098,08	\$ 12.294,55	\$ 13.700,55	\$ 15.031,06
Caso de estudio 18	\$ 9.954,31	\$ 9.954,31	\$ 10.514,31	\$ 10.514,31	\$ 9.733,07
Caso de estudio 19	\$ 28.571,77	\$ 28.571,77	\$ 31.244,77	\$ 32.463,73	\$ 48.968,50
Caso de estudio 20	\$ 48.732,96	\$ 48.732,96	\$ 51.237,04	\$ 51.660,24	\$ 53.269,48
Caso de estudio 21	\$ 21.408,54	\$ 21.408,54	\$ 16.971,69	\$ 16.348,12	\$ 20.213,12
Caso de estudio 22	\$ 10.096,99	\$ 10.096,99	\$ 12.308,71	\$ 14.982,67	\$ 14.982,67
Promedio	\$ 16.754,31	\$ 16.754,31	\$ 19.049,96	\$ 19.984,72	\$ 22.318,47
% de Crecimiento		0,00%	13,70%	4,91%	11,68%

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

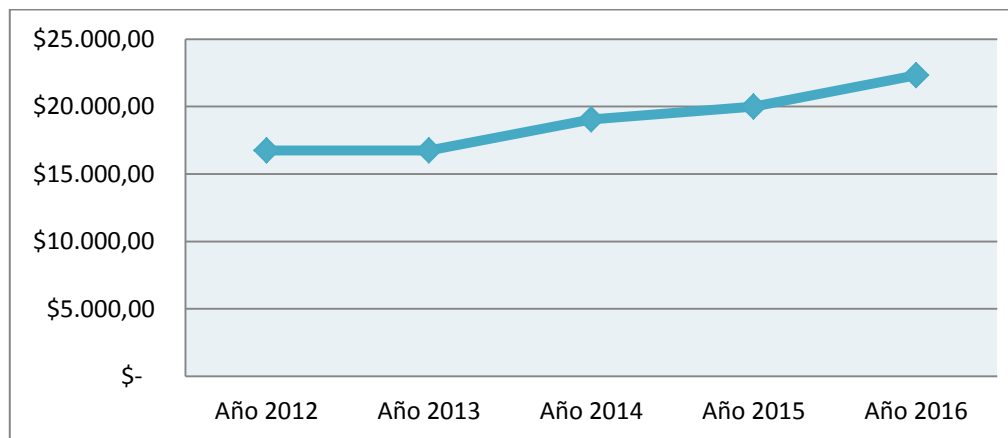


Figura 6. Crecimiento equipo de cómputo – Segmento 4

Las 14 entidades del segmento financiero cuatro durante el periodo 2012-2016 tuvieron un crecimiento porcentual promedio de 7,57% en la cuenta equipo de cómputo.

Entidades reguladas por la Superintendencia de Compañías

Tabla 14
Crecimiento equipo de cómputo – Entidades de la SC.

	Año 2012	Año 2013	Año 2014	Año 2015	Año 2016
Caso de estudio 23	\$ 9.542,66	\$ 10.339,16	\$ 10.339,16	\$ 10.564,16	\$ 10.564,16
Caso de estudio 24	\$ 14.105,91	\$ 14.105,91	\$ 14.105,91	\$ 16.340,96	\$ 22.133,07
Caso de estudio 25	\$ 5.724,10	\$ 7.480,34	\$ 10.458,55	\$ 16.093,96	\$ 18.979,52
Caso de estudio 26	\$ 4.062,02	\$ 4.062,02	\$ 5.795,06	\$ 5.795,06	\$ 8.600,80
Promedio	\$ 8.358,67	\$ 8.996,86	\$ 10.174,67	\$ 12.198,54	\$ 15.069,39
% de Crecimiento		7,64%	13,09%	19,89%	23,53%

Fuente: (Superintendencia de Compañías, 2016)

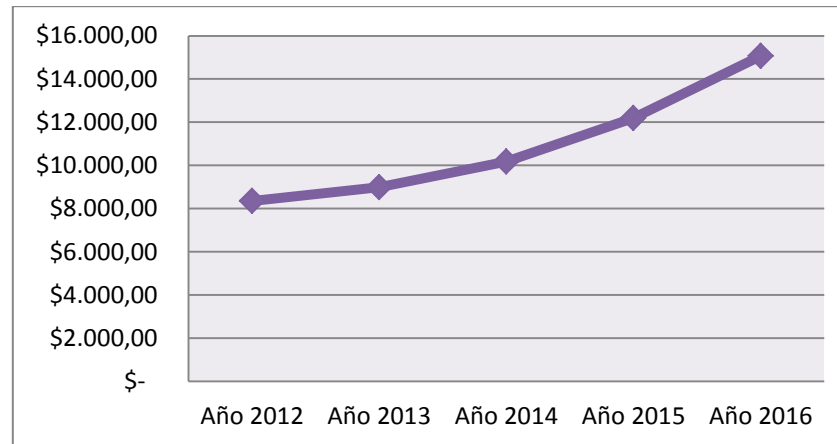


Figura 7. Crecimiento equipo de cómputo– Entidades de la SC

Las 4 entidades reguladas por la Superintendencia de Compañías durante el periodo 2012-2016 tuvieron un crecimiento porcentual promedio de 16,04% en la cuenta equipo de cómputo.

De los resultados obtenidos se deduce que tanto las cooperativas de ahorro y crédito reguladas por la SEPS y el resto de entidades de la Superintendencia de Compañías, presentan en la cuenta equipo de cómputo un crecimiento significativo y es por eso que se fue analizando por grupo de empresas el costo y el beneficio de invertir en herramientas de seguridad y protección de datos.

En cumplimiento al tercer objetivo “Determinar en base a la ISO 27002 los controles de seguridad de la información que utilizan las empresas del sector servicios”. Se formuló preguntas dirigidas a la gerencia y al personal del área de tecnologías de la información, obteniendo resultados confiables de la situación actual de las empresas servicios sobre este tema.

4.3. Análisis de los resultados de la encuesta

1) ¿Qué tipo de políticas de seguridad de la información aplica en la organización?

Tabla 15

Aplicación de Políticas de Seguridad de la Información.

	Políticas de control de acceso y autenticación	Políticas de uso de dispositivos para movilidad	Políticas de uso de controles criptográficos	Políticas de intercambio de información	Políticas de puesto de trabajo despejado y bloqueo de pantalla automático.	Políticas de seguridad de la información para proveedores	Ninguno	Desconoce
Caso Estudio 1	1	1	0	1	1	0	0	0
Caso Estudio 2	1	1	0	1	1	1	0	0
Caso Estudio 3	1	1	1	1	1	1	0	0
Caso Estudio 4	1	0	0	1	0	0	0	0
Caso Estudio 5	1	0	0	0	1	1	0	0
Caso Estudio 6	1	0	0	1	0	1	0	0
Caso Estudio 7	1	0	0	0	1	1	0	0
Caso Estudio 8	1	1	0	1	1	0	0	0
Caso Estudio 9	1	0	0	0	0	0	0	0
Caso Estudio 10	0	0	0	0	0	0	0	1
Caso Estudio 11	1	1	0	1	0	1	0	0
Caso Estudio 12	0	0	0	0	0	0	1	0
Caso Estudio 13	1	0	0	0	0	0	0	0
Caso Estudio 14	1	0	0	0	0	0	0	0
Caso Estudio 15	1	0	0	0	0	0	0	0
Caso Estudio 16	0	0	0	0	0	1	0	0
Caso Estudio 17	0	0	0	1	1	1	0	0
Caso Estudio 18	1	0	0	1	0	0	0	0
Caso Estudio 19	1	1	1	1	1	1	0	0
Caso Estudio 20	0	0	0	1	0	0	0	0
Caso Estudio 21	1	0	0	0	0	0	0	0
Caso Estudio 22	1	0	0	0	0	0	0	0
Caso Estudio 23	1	0	0	1	1	1	0	0
Caso Estudio 24	0	0	0	1	0	0	0	0
Caso Estudio 25	1	0	0	1	0	0	0	0
Caso Estudio 26	1	0	0	1	0	1	0	0
Total Empresas	20	6	2	15	9	11	1	1
%	76,92%	23,08%	7,69%	57,69%	34,62%	42,31%	3,85%	3,85%

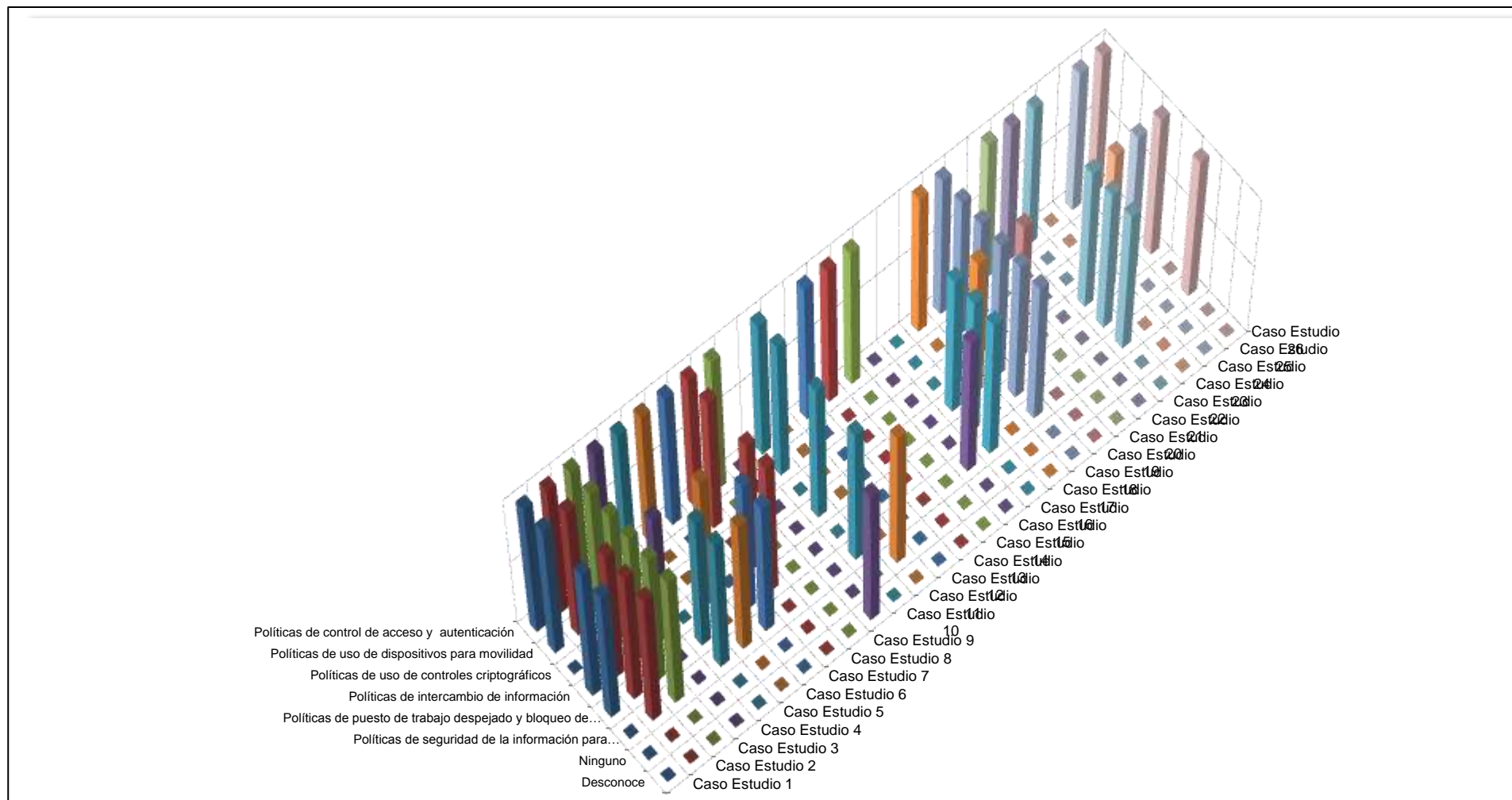


Figura 8. Aplicación de políticas de Seguridad de la Información

Análisis

De las 26 empresas de servicios encuestados el 77% aplican políticas de control de acceso y autenticación, seguido del 58% con políticas de intercambio de información, el 42% sobre seguridad para proveedores, el 35% aplican las políticas de puesto de trabajo despejado y bloqueo de pantalla, posterior al 23% con políticas de uso de dispositivos para movilidad, y apenas el 8% sobre el uso de controles criptográficos, finalmente el 4% no aplica ningún tipo de políticas de la información, lo mismo ocurre que tan solo en una empresa se desconoce si se cuenta con políticas o no.

Al concentrar las respuestas se pudo observar que las políticas de control de acceso y autenticación son mayormente aplicadas en las empresas de servicios, es evidente la importancia de asignar a los empleados una identificación única personal para acceder a los sistemas y demás instalaciones, con el fin de proteger la información manejada por los diferentes usuarios.

2. ¿En función de su organigrama de qué área / departamento depende la seguridad de la información?

Tabla 16

Departamento encargado de la S.I

	Gerencia General / Comité	Tecnología de información	Otro: ¿Cuál?	Servicio de externalización
Caso Estudio 1	0	0	1	0
Caso Estudio 2	1	1	0	0
Caso Estudio 3	0	1	0	0
Caso Estudio 4	0	1	0	0
Caso Estudio 5	0	1	0	0
Caso Estudio 6	0	1	0	0
Caso Estudio 7	1	1	0	0
Caso Estudio 8	0	1	0	0
Caso Estudio 9	0	1	0	0
Caso Estudio 10	0	0	0	1
Caso Estudio 11	1	0	0	1
Caso Estudio 12	1	0	0	1
Caso Estudio 13	1	0	0	1
Caso Estudio 14	1	0	0	1
Caso Estudio 15	0	1	0	0
Caso Estudio 16	1	0	0	1
Caso Estudio 17	1	0	0	1
Caso Estudio 18	1	0	0	0
Caso Estudio 19	0	1	0	0
Caso Estudio 20	1	0	0	1
Caso Estudio 21	0	1	0	0
Caso Estudio 22	1	0	0	1
Caso Estudio 23	1	0	0	1
Caso Estudio 24	0	0	1	0
Caso Estudio 25	0	0	1	0
Caso Estudio 26	1	0	0	1
Total Empresas	13	11	3	11
%	50%	42%	12%	42%

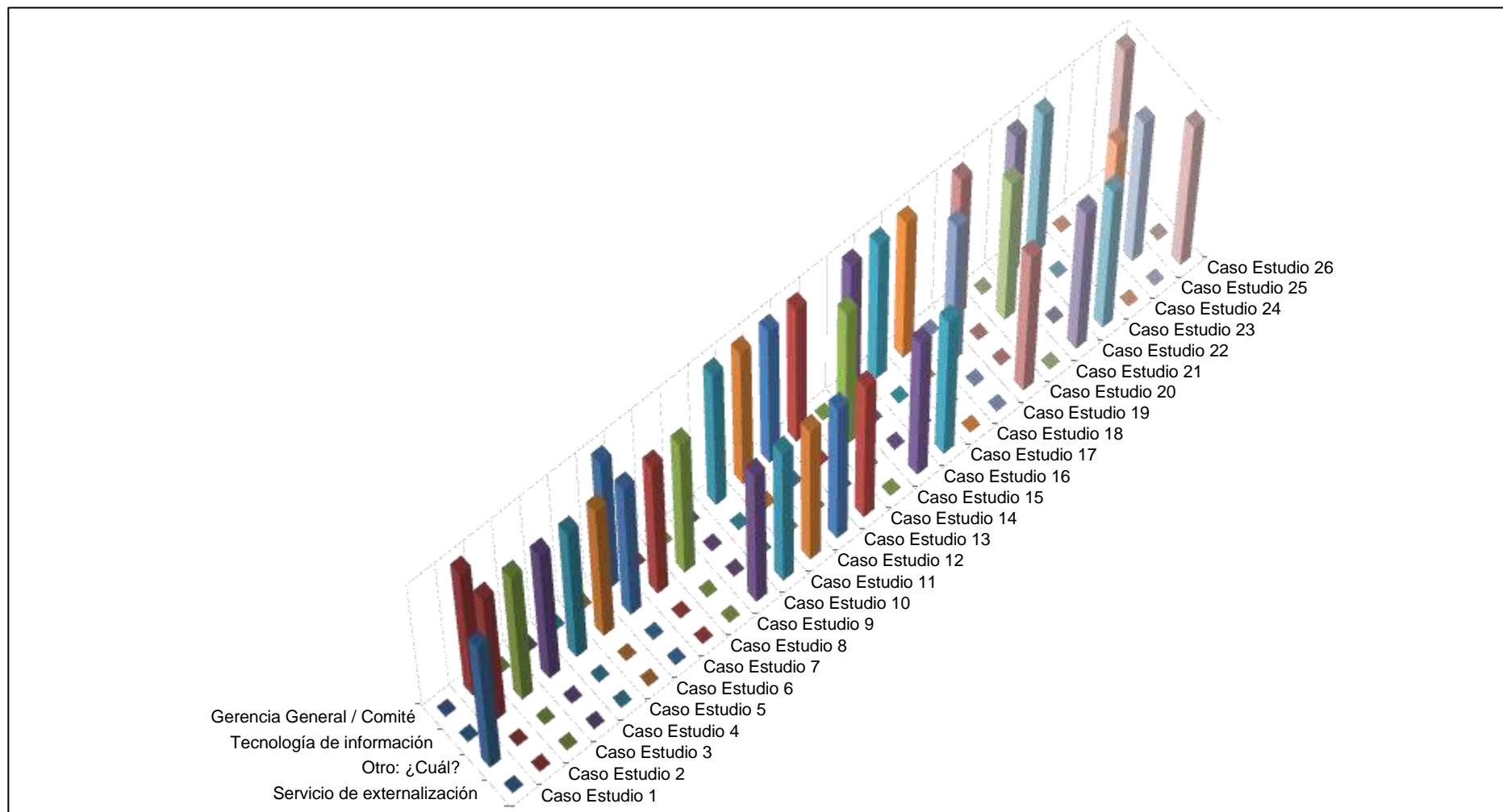


Figura 9. Departamento encargado de la S.I

Análisis

Del total de encuestados, el 50% establece a la Gerencia General como responsable de seguridad de la información, mientras que el 42% es del departamento de Tecnología, el mismo dato sucede con el apoyo de servicios de externalización, por último el 12% cuentan con departamentos diferentes encargados propiamente de seguridad de la información, es así como también se presentan los departamentos de Sistemas de Gestión.

Estos datos muestran que en la mayor parte de empresas es la gerencia encargada de proteger la información, pero algunas entidades van de la mano con los servicios de externalización, hecho que ocurre por lo general en las empresas pequeñas como es el caso de las que pertenecen al segmento financiero cuatro.

3. ¿El departamento encargado de seguridad de la información se ocupa de dar de baja a los accesos de los empleados una vez que termine el contrato laboral?

Tabla 17

Accesos dados de baja

Opciones	Frecuencia	Porcentaje válido
No	6	23,08%
Si	20	76,92%
Total	26	100,00%

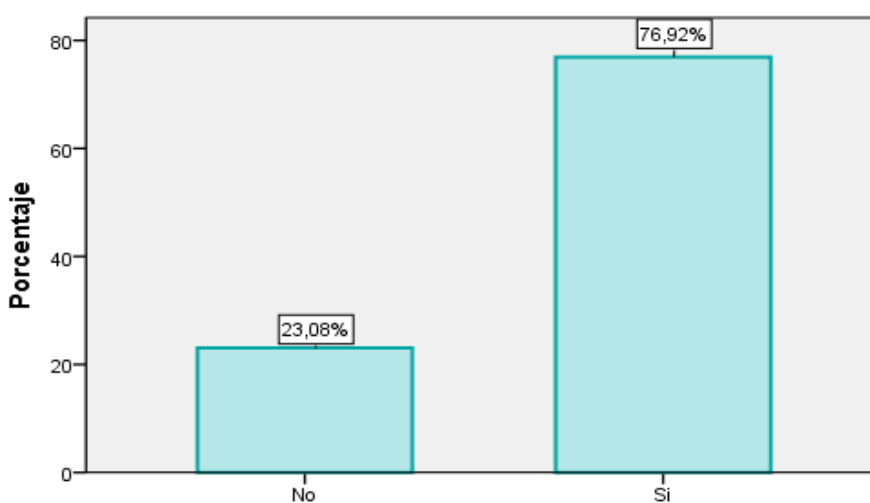


Figura 10. Accesos dados de baja

Análisis

Del total de empresas encuestadas reguladas por los respectivos organismos de control el 76,92% indican que el departamento encargado de seguridad de la información si se ocupa de dar de baja a los accesos de los empleados una vez que termine el contrato laboral, mientras que el 23,08% de las entidades no dan de baja a los accesos que tienen los empleados a los sistemas y servicios de información cuando se da lugar a la finalización del empleo o contrato de trabajo.

Cabe considerar que este control no lo aplican la mitad de las entidades correspondientes a la Superintendencia de compañías lo cual implica un riesgo para la entidad ya que puede darse lugar al uso indebido de la información al cual tienen acceso.

4. ¿Actualmente se aplica herramientas de Seguridad de la información en la entidad?

Tabla 18

Herramientas de S.I

Opciones	Frecuencia	Porcentaje válido
No	2	7,69%
Si	24	92,31%
Total	26	100,00%

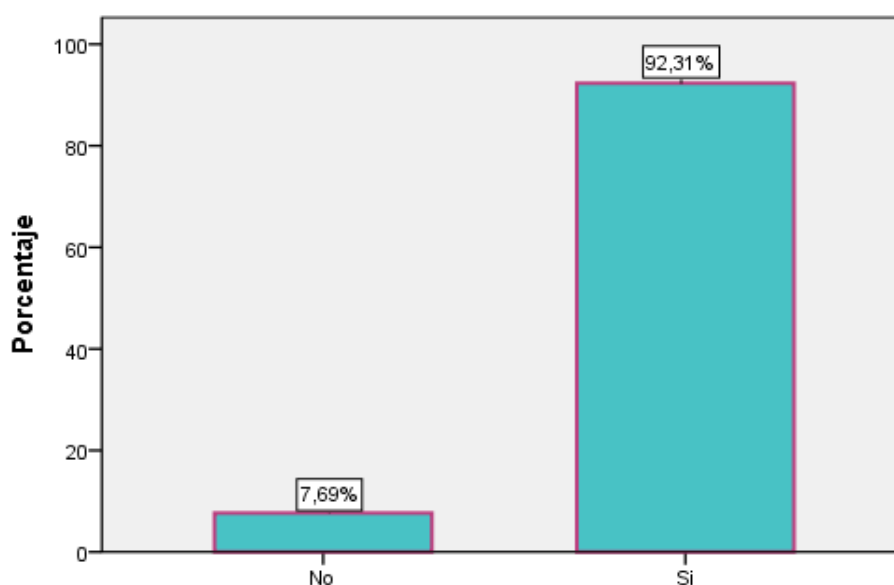


Figura 11. Aplicación de Herramientas de S.I

Análisis

De la totalidad de empresas encuestadas reguladas por los respectivos organismos de control se observa los siguientes resultados, donde un 92,31% manifiesta que actualmente si aplican herramientas de seguridad de la información en la entidad mientras que solo el 7,69% no tienen ninguna herramienta para proteger la seguridad de la información en la entidad, dentro de este resultado se evidencia únicamente a las cooperativas de ahorro y crédito del segmento cuatro sin embargo viene a constituir un porcentaje mínimo.

4) Si su respuesta es sí ¿Cuáles son las herramientas o mecanismo de seguridad que se aplican en la entidad para proteger la información?

Tabla 19

Herramientas de S.I

	Uso de Antivirus	Uso de Antimalware	Uso de Antispyware	Uso de Firewall	Actualizaciones de sistema	Ninguna
Caso Estudio 1	1	1	0	1	0	0
Caso Estudio 2	1	1	1	1	1	0
Caso Estudio 3	1	1	0	1	1	0
Caso Estudio 4	1	1	1	1	1	0
Caso Estudio 5	1	1	1	0	1	0
Caso Estudio 6	1	0	0	1	0	0
Caso Estudio 7	1	0	0	1	0	0
Caso Estudio 8	1	1	1	1	1	0
Caso Estudio 9	0	1	0	0	0	0
Caso Estudio 10	0	0	0	1	0	0
Caso Estudio 11	1	0	0	0	0	0
Caso Estudio 12	0	0	0	0	0	1
Caso Estudio 13	1	0	0	1	0	0
Caso Estudio 14	0	0	0	0	0	1
Caso Estudio 15	1	0	0	0	0	0
Caso Estudio 16	1	0	0	0	1	0
Caso Estudio 17	1	0	0	1	0	0
Caso Estudio 18	1	0	0	0	0	0
Caso Estudio 19	1	1	1	1	0	0
Caso Estudio 20	1	0	0	0	1	0
Caso Estudio 21	1	1	0	1	0	0
Caso Estudio 22	0	0	0	0	0	1

CONTINUA 

Caso Estudio 23	1	0	0	0	1	0
Caso Estudio 24	1	0	0	0	0	0
Caso Estudio 25	1	0	0	0	0	0
Caso Estudio 26	1	0	0	0	0	0
Total Empresas	21	9	5	12	8	3
%	81%	35%	19%	46%	31%	12%

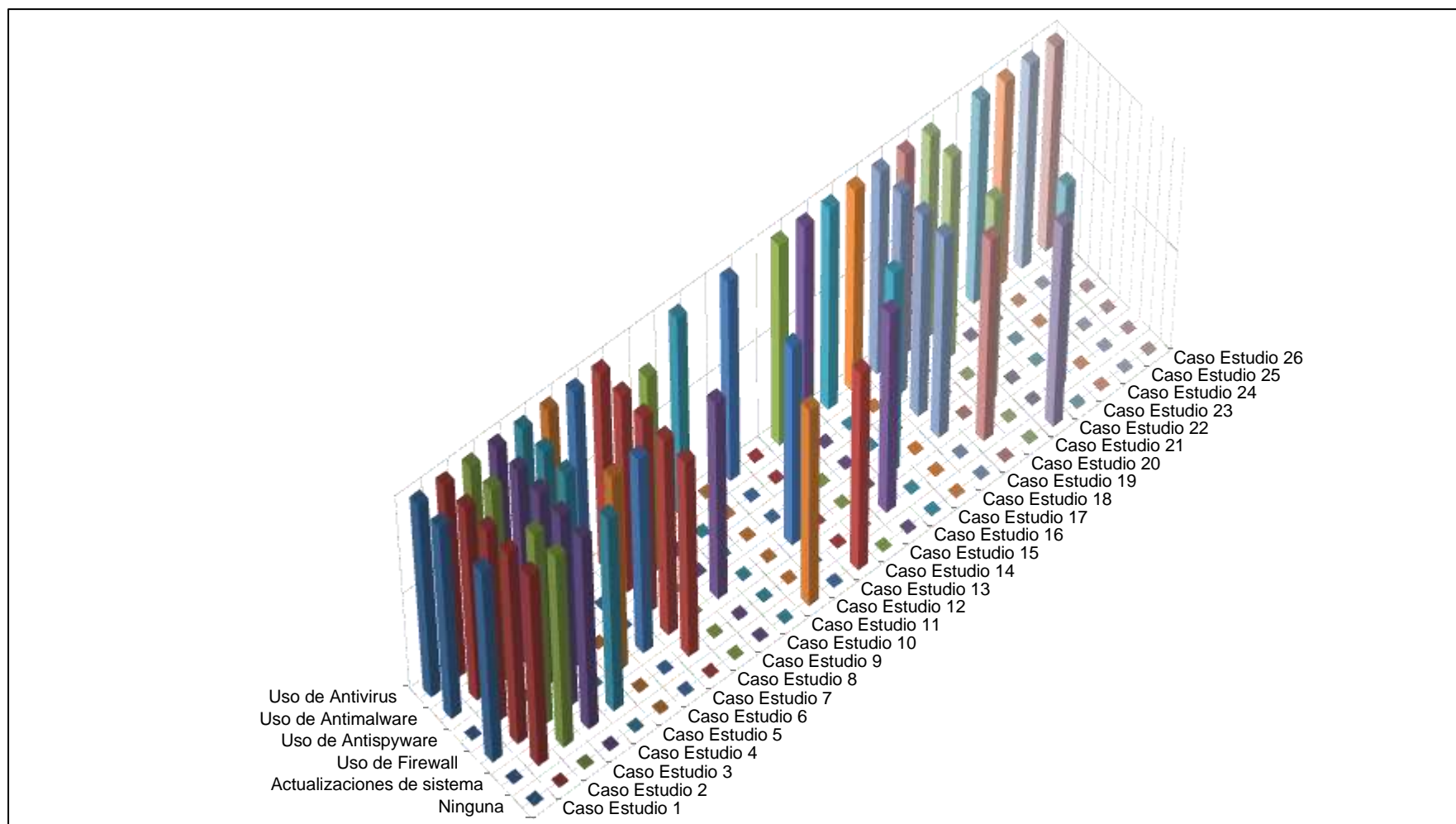


Figura 12. Herramientas de S.I

Análisis

En base a los resultados y en relación a las herramientas o mecanismos de seguridad utilizados para proteger la información, demuestran que del total de encuestados, el 81% utilizan antivirus, el 46% Firewall, el 35% antimalware, el 31% como medidas de seguridad aplican las actualizaciones del sistema, el 19% antispyware, por último el 12% no utilizan ningún tipo de herramienta de seguridad de la información.

En la encuesta realizada las empresas que no cuentan con herramientas de seguridad una de las razones es por el colapso del sistema que manejan o simplemente por desconocimiento, así también en el sector servicios, el antivirus y el Firewall son mayormente utilizados para proteger la información contenida en los ordenadores.

5. ¿Hacia dónde orientaría la inversión de Seguridad de la información en la empresa?

Tabla 20

Inversión en Seguridad de la Información

	Cumplimiento de políticas internas	Capacitación	Cumplimiento de regulaciones	Certificación de estándares de seguridad	Incremento de la estructura del personal	Hardware	Software	Tercerización de las actividades de seguridad
Caso Estudio 1	1	0	1	0	0	1	1	0
Caso Estudio 2	0	0	1	0	0	0	0	0
Caso Estudio 3	1	1	0	0	0	1	1	0
Caso Estudio 4	1	0	1	1	1	1	0	0
Caso Estudio 5	1	1	1	0	0	1	1	0
Caso Estudio 6	1	1	1	0	0	0	1	0
Caso Estudio 7	1	0	0	1	0	0	0	0
Caso Estudio 8	1	1	1	1	1	1	1	0
Caso Estudio 9	0	0	0	1	0	0	0	0
Caso Estudio 10	0	0	0	0	0	1	0	0
Caso Estudio 11	1	1	0	1	0	1	1	0
Caso Estudio 12	0	1	0	0	1	1	1	0
Caso Estudio 13	1	1	1	0	0	1	1	1
Caso Estudio 14	0	0	0	1	0	0	0	0
Caso Estudio 15	0	1	0	0	0	0	0	0
Caso Estudio 16	1	0	0	0	0	0	1	0
Caso Estudio 17	1	1	0	0	1	0	1	0
Caso Estudio 18	1	1	0	0	0	0	0	0
Caso Estudio 19	0	0	0	0	0	1	1	0
Caso Estudio 20	1	1	0	1	1	1	1	0
Caso Estudio 21	1	0	0	1	1	1	0	0
Caso Estudio 22	0	0	1	0	0	1	1	0
Caso Estudio 23	1	1	0	0	1	0	0	0
Caso Estudio 24	1	1	0	0	0	0	1	0
Caso Estudio 25	1	0	1	0	0	0	0	0
Caso Estudio 26	0	0	0	1	0	0	1	0
Total Empresas	17	13	9	9	7	13	15	1
%	65%	50%	35%	35%	27%	50%	58%	4%

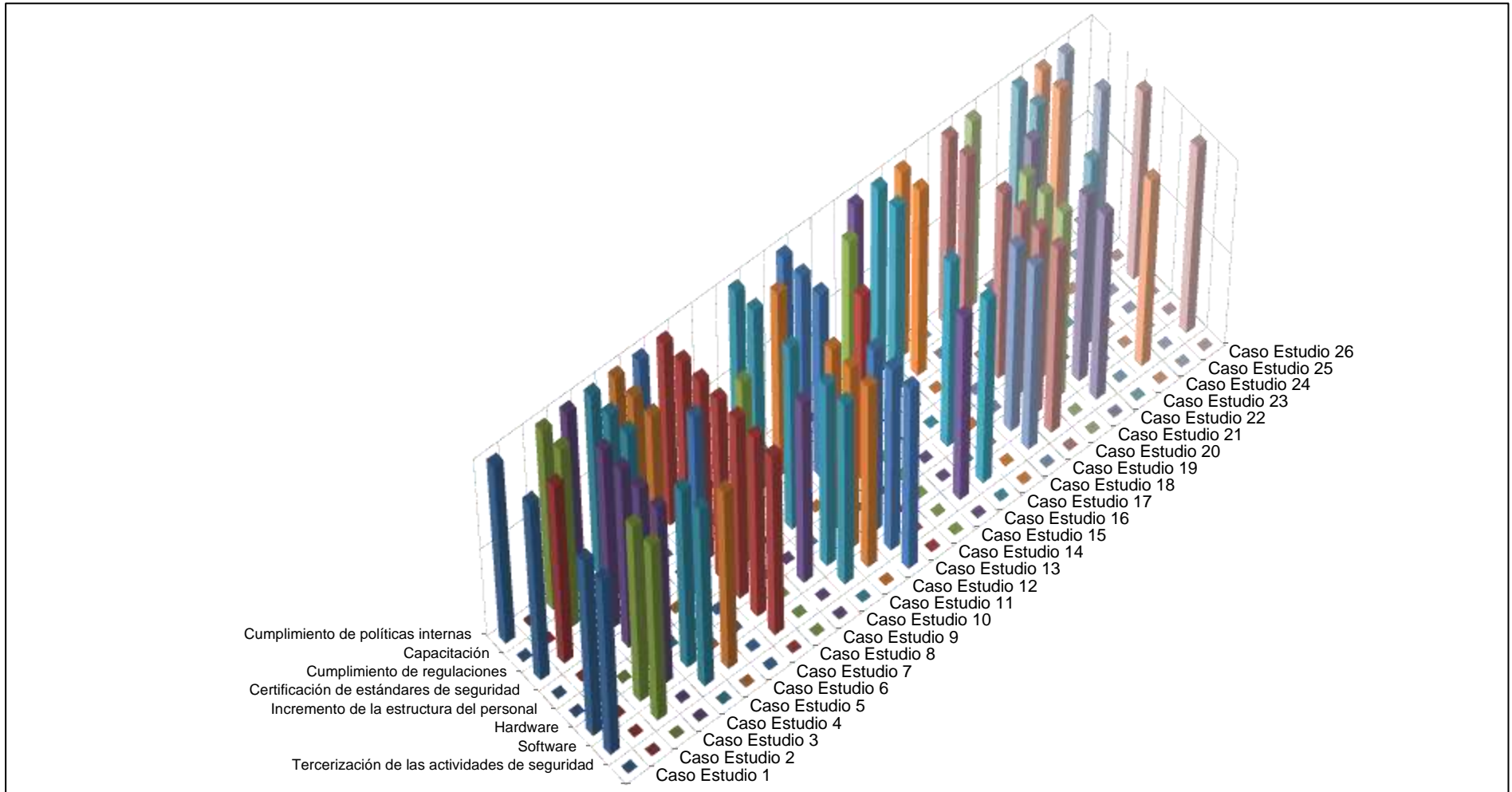


Figura 13. Inversión en Seguridad de la Información

Análisis

Según los resultados presentados en la tabla, el 65% buscan invertir en el cumplimiento de políticas internas, seguido del 58% en software, el 50% están realmente interesados invertir en capacitación y en Hardware, el 35% desean invertir en cumplimiento de regulaciones y en la certificación de estándares, el 27% requieren incrementar la estructura del personal para la seguridad de la información, finalmente el 4% se inclina a la tercerización de las actividades de seguridad.

Al concentrar las respuestas se pudo observar que la mayor parte de empresas orientarían la inversión de Seguridad de la información en el cumplimiento de políticas internas, que básicamente es el conjunto de normas documentadas que deben ser divulgadas, entendidas y acatadas por todos los miembros de la organización.

6) ¿Cuáles son los incidentes /brechas de seguridad de la información más comunes que se han producido anualmente en el periodo 2012 - 2016?

Tabla 21

Incidentes y brechas de Seguridad de la Información

	Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)	Modificación o eliminación no autorizada de datos	Robo / acceso a la información	Interrupción prolongada en un sistema o servicio de red	Acceso o intento de acceso no autorizado a un sistema informático	Ingeniería social, fraude o phishing	Destrucción no autorizada de información	Robo de equipos	Uso indebido de información crítica	Ninguno
Caso Estudio 1	1	0	0	0	0	1	0	0	0	0
Caso Estudio 2	1	0	0	0	0	0	0	0	0	0
Caso Estudio 3	0	0	0	0	0	1	0	0	1	0
Caso Estudio 4	1	1	0	0	0	0	0	1	0	0
Caso Estudio 5	0	1	0	0	0	0	0	1	1	0
Caso Estudio 6	0	0	0	1	0	0	0	0	0	0
Caso Estudio 7	1	0	0	0	0	0	1	1	1	0
Caso Estudio 8	0	0	0	0	0	0	0	0	0	1
Caso Estudio 9	0	0	0	1	0	0	0	0	0	0
Caso Estudio 10	1	0	0	0	0	0	0	0	0	0
Caso Estudio 11	1	0	0	0	1	0	0	0	0	0
Caso Estudio 12	1	0	0	0	0	0	0	0	0	0
Caso Estudio 13	0	0	0	0	0	0	0	0	0	1
Caso Estudio 14	1	0	0	0	0	0	0	0	0	0
Caso Estudio 15	1	0	0	0	0	0	0	0	0	0
Caso Estudio 16	1	0	0	0	0	0	0	0	0	0
Caso Estudio 17	1	0	0	1	0	0	0	0	1	0
Caso Estudio 18	0	0	0	0	0	1	0	0	0	0
Caso Estudio 19	1	0	0	0	1	0	1	0	0	0
Caso Estudio 20	0	0	0	1	0	0	0	0	0	0
Caso Estudio 21	0	0	0	0	0	0	0	0	1	0
Caso Estudio 22	1	0	0	0	0	0	0	0	1	0
Caso Estudio 23	1	0	1	1	0	0	0	1	0	0
Caso Estudio 24	1	0	1	0	0	0	0	0	0	0
Caso Estudio 25	0	0	0	0	0	0	0	1	0	0
Caso Estudio 26	0	0	0	0	1	0	0	0	1	0
Total Empresas	15	2	2	5	3	3	2	5	7	2
%	58%	8%	8%	19%	12%	12%	8%	19%	27%	8%

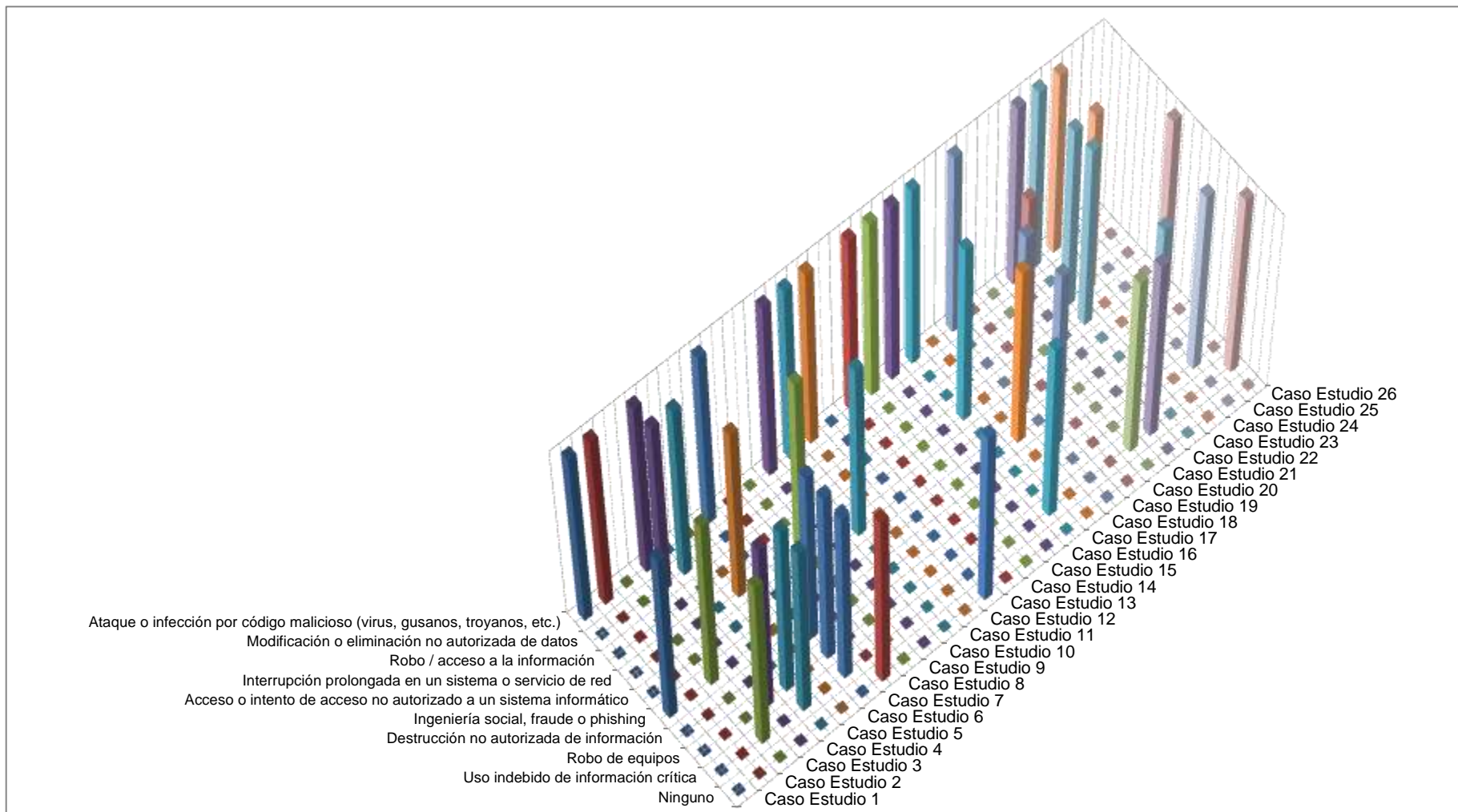


Figura 14. Incidentes y Brechas de Seguridad de la Información

Análisis

En base a los resultados presentados en la tabla, con relación a incidentes o brechas de seguridad de la información, el 58% de empresas encuestadas han sufrido de Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.), el 27% por el uso indebido de información crítica, el 19% han sido afectados con la interrupción prolongada en un sistema o servicio de red y el robo de equipos, seguido del 12% que han identificado accesos o intento de accesos no autorizados a un sistema informático, en un mismo porcentaje son las empresas que han sufrido de ingeniería social, fraude o phishing, finalmente el 8% han detectado ataques por modificación o eliminación no autorizada de datos, y por robo / acceso a la información y su destrucción no autorizada, apenas 2 empresas no han sufrido de ningún tipo de ataque a la seguridad de la información.

La pregunta demuestra que casi todas las empresas de alguna u otra forma se han visto afectadas con relación a incidentes o brechas de seguridad de la información, es evidente que más de la mitad han sufrido de ataques por códigos maliciosos tal es el caso de los virus.

7. ¿Cuál es el costo que le representó enmendar los problemas de seguridad de la información identificados en la empresa?

Tabla 22

Costos incidentes de S.I

Opciones	Frecuencia	Porcentaje válido
Hasta \$9.000	9	34,62%
Hasta \$12.000	5	19,23%
Hasta \$15.000	4	15,38%
Hasta \$20.000	1	3,85%
No aplica	7	26,92%
Total	26	100;00%

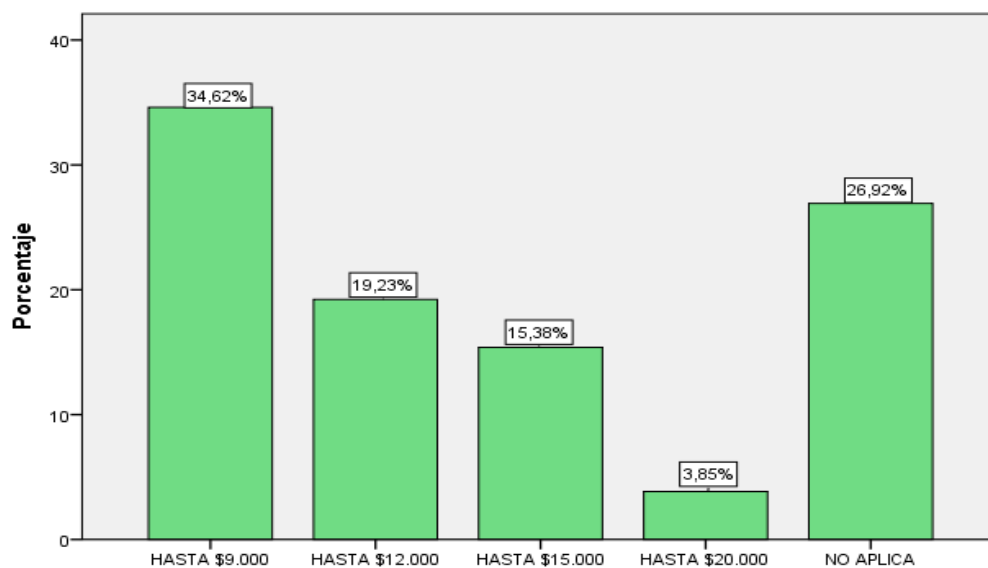


Figura 15. Costos incidentes de S.I

Análisis

En relación a los incidentes y problemas de seguridad más comunes producidos anualmente, que han afectado a las empresas reguladas por los respectivos organismos de control en los últimos cuatro años, se evidencia cual fue el promedio del costo que representó para reparar los daños, en este sentido un 34.62% indica un costo de hasta \$9.000 dólares mayormente en las cooperativas del segmento cuatro, seguido por un 26.92% que indica que no le represento ningún costo, por otro lado un 19,23% revela que el promedio del costo fue de hasta \$12.000 aquí se encuentran las entidades del segmento tres, mientras que el 15.38% indica que le representó un costo de hasta \$15.000 dentro de este porcentaje se encuentran entidades del segmento dos y las entidades reguladas por la S.C. y el 3.85% de los encuestados menciona que tuvo un costo hasta los \$20.000 correspondiendo este valor a una cooperativa de ahorro y crédito del segmento uno.

8) ¿Cuánto es el monto de inversión, que fue asignado para la seguridad de la información, durante el periodo 2012 al 2016?

Tabla 23

Presupuesto anual S.I

Opciones	Frecuencia	Porcentaje válido
Menos de \$5.000	11	42,31%
De \$5.000 a \$ 15.000	7	26,92%
De \$15.000 a \$30.000	4	15,38%
De \$30.000 a \$40.000	2	7,69%
Mayores a \$40.000	1	3,85%
No aplica	1	3,85%
Total	26	100,00%

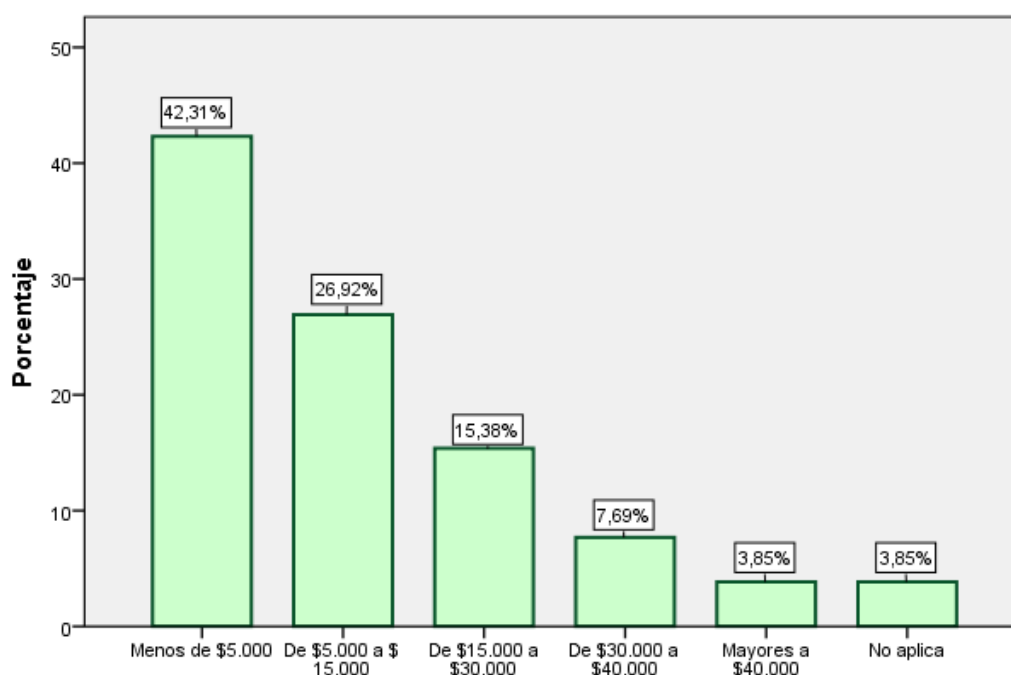


Figura 16. Presupuesto anual de S.I

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control se evidencia que un 42.31% asignaron como promedio un presupuesto anual para herramientas de S.I menos de \$5.000 dólares correspondiendo este valor a la mayoría de entidades del segmento cuatro y empresas reguladas por la Superintendencia de Compañías, así también durante ese periodo un 26.92% establece que invirtió un

presupuesto que va de \$5.000 a \$15.000 ubicándose aquí en su mayoría entidades del segmento dos y tres, el 15.38% indica que el promedio del presupuesto que asigno va desde los \$15.000 a \$30.000, sin embargo también es importante analizar que para el 7.69% de las empresas encuestadas el presupuesto que se asignó durante ese periodo se ubica entre \$30.000 y \$40.000 misma que corresponde a una entidad del segmento dos y tres, y para el 3.85% el presupuesto que se asignó es mayores a \$40.000 dólares aquí se ubica una entidad del segmento uno, finalmente para el 3.85% cabe indicar que no se asignó ningún presupuesto para esta actividad este porcentaje hace referencia a una entidad del segmento cuatro.

9) ¿Se aceptan y se firman los términos y condiciones del contrato de empleo y/o confidencialidad antes o después iniciar sus labores?

Tabla 24

Términos y condiciones Contrato laboral

Opciones	Frecuencia	Porcentaje válido
Antes	23	88,46%
Después	2	7,69%
No aplica	1	3,85%
Total	26	100,00%

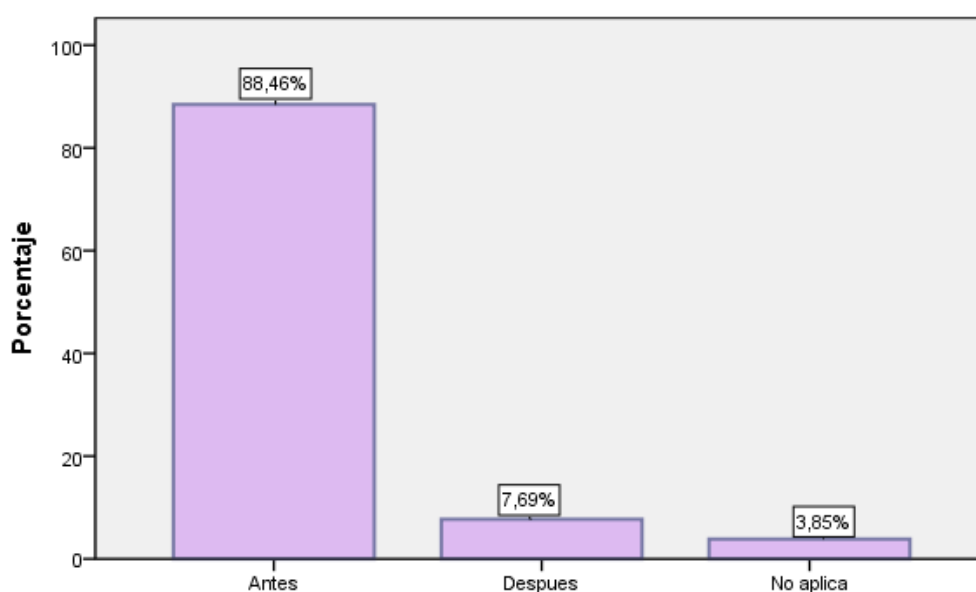


Figura 17. Términos y condiciones Contrato Laboral

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control se evidencia que el 88.46% acepta y firma antes los términos y condiciones del Contrato laboral, mientras que el 7.69% de las empresas acepta y firma después, seguido por el 3.85% que no realiza esta actividad respecto a los acuerdos sobre términos y condiciones del contrato laboral, en este caso este porcentaje se enfoca a una empresa del sector de alojamiento regulada por la Superintendencia de compañías que no aplica el contrato laboral debido a que son empleados con más de 35 años de servicio y en ese tiempo el contrato en si más se basó en la confianza que tenían los dueños de la hostería con personas vecinos o familiares de los alrededores del lugar donde se ubica esta empresa mismos que fueron contratados de una manera informal para laborar en el lugar.

9) ¿Se aceptan y se firman los términos y condiciones del contrato de empleo y/o confidencialidad antes o después de iniciar sus labores?

Tabla 25

Términos y condiciones acuerdos confidencialidad

Opciones	Frecuencia	Porcentaje válido
Antes	16	61,54%
Después	7	26,92%
No aplica	3	11,54%
Total	26	100,00%

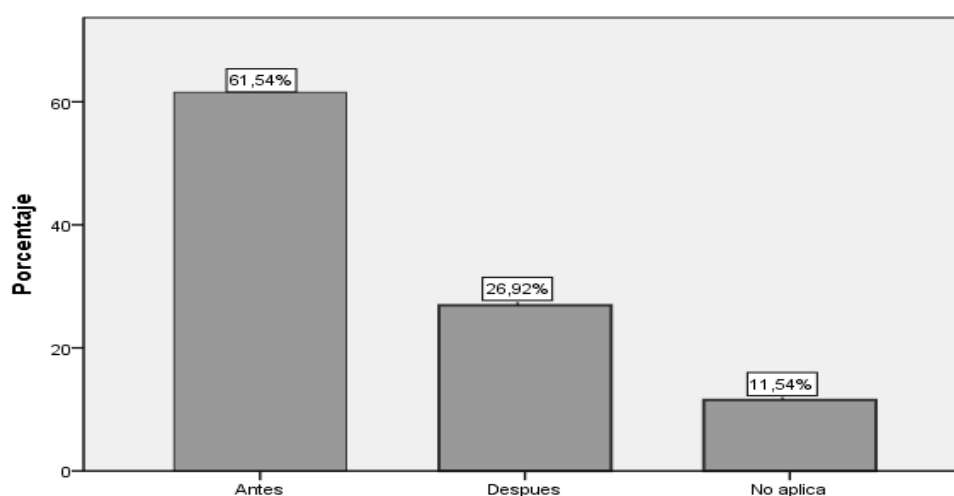


Figura 18. Términos y condiciones acuerdo confidencialidad

Del total de entidades encuestadas reguladas por los respectivos organismos de control se evidencia que el 61.54% acepta y firma antes los términos y condiciones de acuerdos de confidencialidad, mientras que el 26.92% de las empresas acepta y firma después, por otro lado el 11,54% correspondiente a dos empresas reguladas por la Superintendencia de Compañías y una entidad del segmento cuatro no responsabiliza al empleado sobre los términos y condiciones de acuerdo de confidencialidad.

Actualmente este es un aspecto muy importante a considerar en los contratos con los empleados de modo que mediante el acuerdo de confidencialidad se responsabiliza al trabajador sobre la custodia de la información que maneja y en caso de no acatar dicha norma se aplicará sanciones respectivas.

10. ¿Cuál es el tipo de información que mayormente maneja?

Tabla 26

Tipo de información

	Confidencial	Uso interno	Público
Caso Estudio 1	1	0	0
Caso Estudio 2	1	1	0
Caso Estudio 3	0	1	0
Caso Estudio 4	1	0	0
Caso Estudio 5	1	0	0
Caso Estudio 6	0	1	0
Caso Estudio 7	0	1	0
Caso Estudio 8	1	1	1
Caso Estudio 9	1	0	0
Caso Estudio 10	1	0	0
Caso Estudio 11	0	0	1
Caso Estudio 12	0	1	0
Caso Estudio 13	1	0	0
Caso Estudio 14	0	1	0
Caso Estudio 15	1	0	0
Caso Estudio 16	0	1	0
Caso Estudio 17	1	0	0
Caso Estudio 18	0	1	0
Caso Estudio 19	0	1	0
Caso Estudio 20	0	1	0
Caso Estudio 21	0	1	0
Caso Estudio 22	1	1	0
Caso Estudio 23	1	1	0
Caso Estudio 24	0	1	0
Caso Estudio 25	0	1	0
Caso Estudio 26	0	1	0
Total Empresas	12	17	2
%	46%	65%	8%

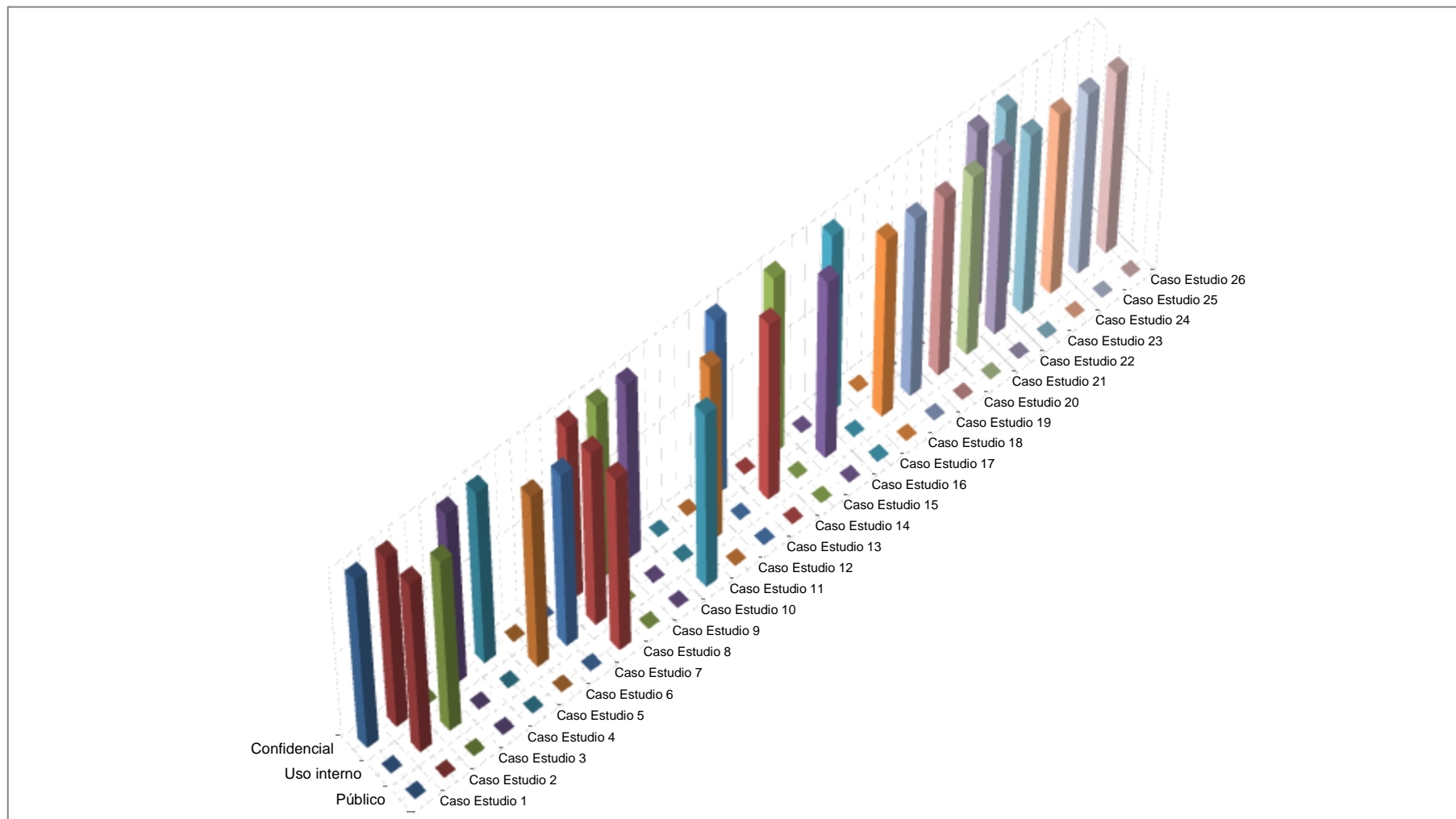


Figura 19. Tipo de información

Análisis

Del total de encuestados, el 65% manejan el tipo de información de uso interno, el 46% utilizan información de tipo confidencial o reservado, por último tan solo 2 empresas que equivale al 8% la información es pública.

Al clasificar la información, ayuda a las empresas enfocar sus esfuerzos en la gestión de información más crítica, permitiendo identificar los riesgos que pueden llegar a tener más relevancia para la empresa y a su vez determinar los controles apropiados y acordes a su realidad. La clasificación de la información además puede producir ahorros significativos ya que garantiza eficiencia en la administración de los recursos y efectividad en su implementación.

11) ¿Se cuenta con controles criptográficos, como por ejemplo el uso de certificados digitales u otros programas para el cifrado de datos?

Tabla 27

Controles criptográficos

Opciones	Frecuencia	Porcentaje válido
No	16	61,54%
Si	10	38,46%
Total	26	100,00%

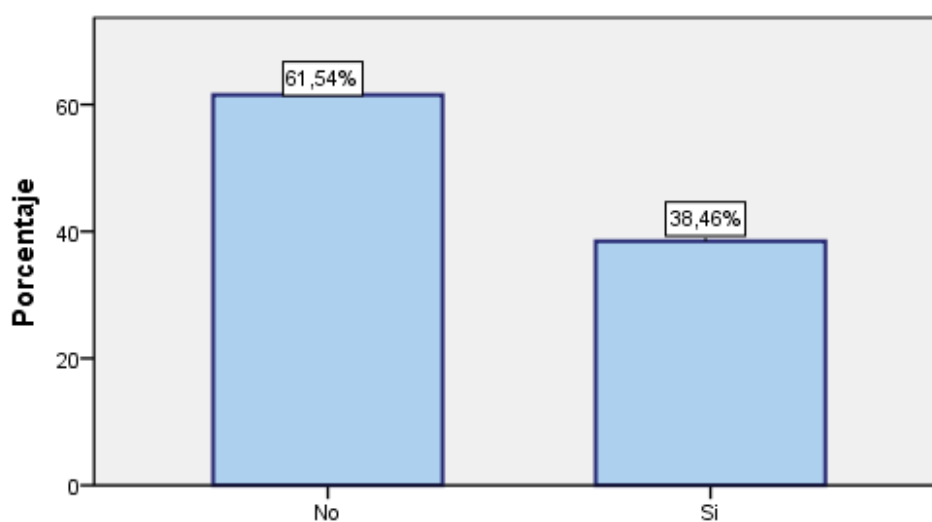


Figura 20. Controles criptográficos

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control, los resultados observados indican que el 38,46% si cuenta con controles criptográficos para el cifrado de datos, mientras que el 61,54% de las empresas manifiesta que no utilizan ningún tipo de control criptográfico para el cifrado de datos, correspondiendo la mayoría de este porcentaje a las cooperativas de ahorro y crédito del segmento tres, cuatro y entidades reguladas por la Superintendencia de Compañías, por lo tanto esta parte de los encuestados no tiene garantizado la protección de la autenticidad, confidencialidad e integridad de la información sensible o crítica para la entidad.

12. ¿Se cuenta con un inventario de activos de la información?

Tabla 28

Activos información

Opciones	Frecuencia	Porcentaje válido
No	4	15,38%
Si	22	84,62%
Total	26	100,00%

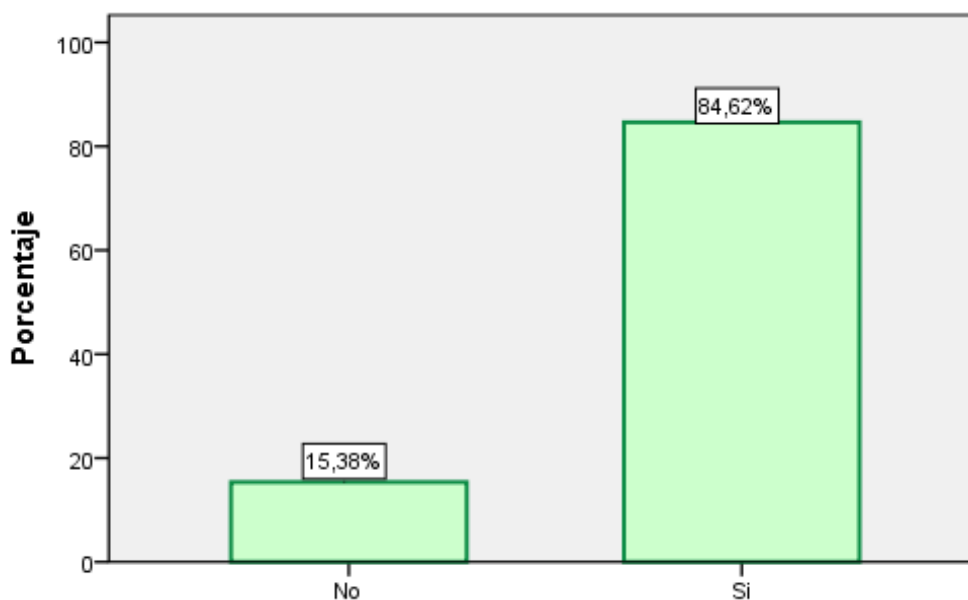


Figura 21. Activos de la información

Análisis

Del total de encuestados reguladas por los respectivos organismos de control, la mayor parte representada por un porcentaje de 84,62% indica que la entidad dispone de un inventario de activos de la información como recursos de información, recursos de software, activos físicos, servicios informáticos y de comunicaciones (iluminación, calefacción, energía eléctrica, etc.), mientras que el 15,36% no tienen inventariado sus activos de la información por lo tanto no tienen un conocimiento de los activos que poseen, en este sentido estas entidades no podrían dar un tratamiento adecuado a cada uno de estos activos con medidas que protejan a los mismos de las incidencias o fallas en la seguridad.

13.¿Posee algún método o programa para borrar la información confidencial de los medios magnéticos, cuando se requiere deshacerse del medio o equipo, enviar a servicio técnico o devolver a su proveedor?

Tabla 29

Método_ programa borrado Información

Opciones	Frecuencia	Porcentaje válido
No	15	57,69%
Si	11	42,31%
Total	26	100,00%

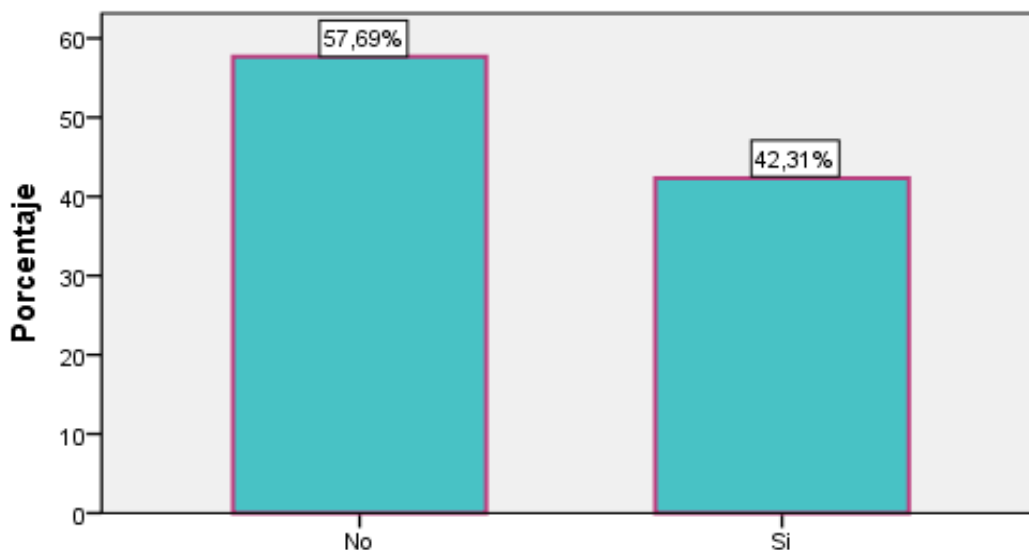


Figura 22. Método _ programa borrado información

Análisis

Del total de las entidades encuestadas reguladas por los respectivos organismos de control de los resultados obtenidos se observa que el 42,31% si tiene un método o programa para borrar la información confidencial de los medios magnéticos, cuando se requiere deshacerse del medio o equipo, enviar a servicio técnico o devolver a su proveedor, mientras que el 57,69% no cuenta con esta herramienta y la mayor parte son entidades que corresponden al segmento cuatro, en este caso es importante indicar que la eliminación inadecuada de estos activos de la información una vez que cumplan con su ciclo final de vida de acuerdo a los regulaciones establecidas, puede dar lugar a la causa raíz de que ocurran ciertos incidentes de Seguridad de la Información.

El borrado parece ser un proceso sencillo sin embargo no es así ya que el sistema operativo no proporciona un borrado seguro, solamente se produce el falso borrado que es muy conveniente en términos de costos, es decir que cuando se elimina un archivo del disco duro, este no desaparece físicamente del soporte de almacenamiento, sino que se modifica su etiqueta identificadora para indicar al sistema de archivos que el espacio que ocupa está disponible para que, en caso de necesitarlo, aloje allí los datos de otro archivo, por lo tanto con algún software se podría recuperar y acceder fácilmente a la información que contenía tales archivos.

14. ¿El sistema registra los intentos de accesos fallidos y exitosos?

Tabla 30

Registro de intento de accesos

Opciones	Frecuencia	Porcentaje válido
No	6	23,08%
Si	20	76,92%
Total	26	100,00%

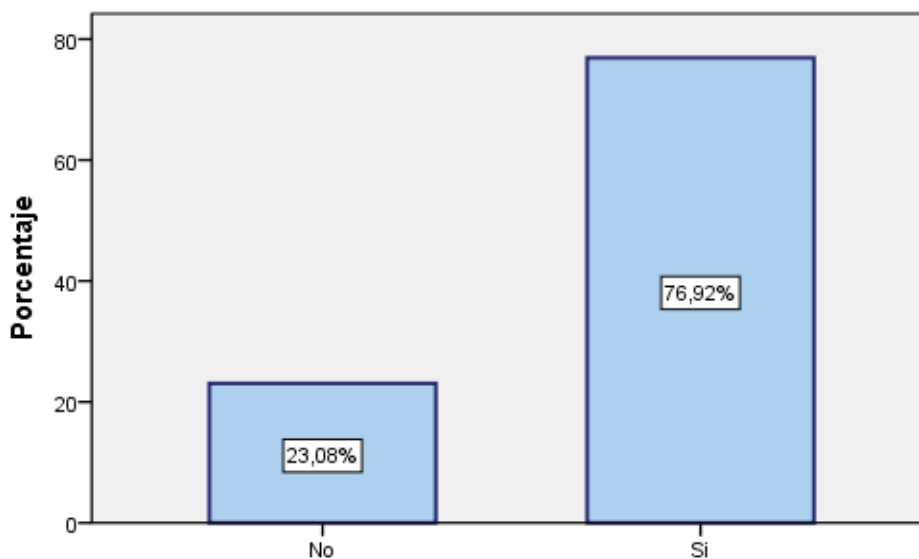


Figura 23. Registro e intentos de accesos

Análisis

Del total de empresas encuestadas reguladas por los respectivos organismos de control, de los resultados obtenidos se puede observar que el 76.92% el sistema si registra los intentos de accesos fallidos y exitosos, mientras que el 23,08% el sistema no realiza esta acción, dentro de este porcentaje están las entidades reguladas por la Superintendencia de Compañías y el resto pertenece a las cooperativas de ahorro y crédito del segmento cuatro que no cumplen con este control.

Las empresas al no tener registros de actividad de los sistemas (logs) no se puede monitorizar el estado del riesgo en los sistemas o la detección de intrusos, hay que considerar que al contar con este control como mínimo los logs deben registrar información intentos de acceso al sistema tanto exitosos como fallidos, identidad del usuario, fecha de intento de acceso, tiempo de cada intento de entrada, fecha y tiempo de salida del sistema del sistema, actividades y funciones ejecutadas por el usuario que ha accedido, cuya información facilita también los registros de auditoria y ayudar a los responsables de la S.I a mantener controlado ciertos aspectos.

15. ¿Tiene segmentada la red de la empresa de acuerdo algún criterio?

Tabla 31

Segmentación de Red

Opciones	Frecuencia	Porcentaje válido
No	14	53,85%
Si	12	46,15%
Total	26	100,00%

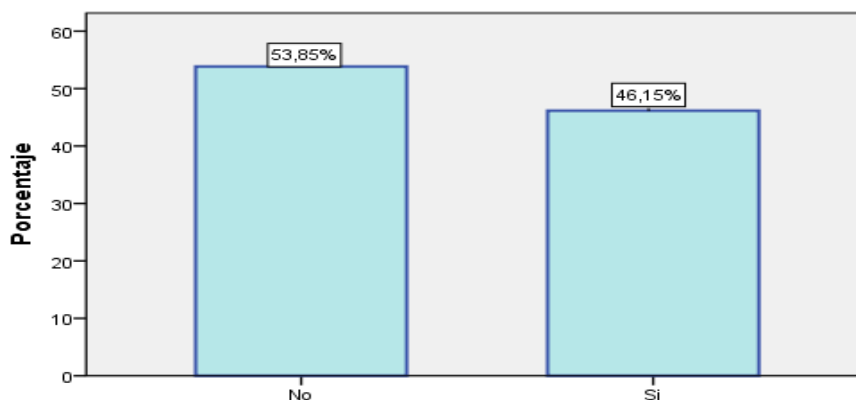


Figura 24. Segmentación de red

Análisis

Del total de entidades encuestas reguladas por los respectivos organismos de control según los resultados obtenidos se observa que el 46.15% si tiene segmentada la red de la empresa, sin embargo el 53,85% de las empresas encuestadas indican que no tienen segmentada la red, dentro de este porcentaje se puede evidenciar a la mayoría de cooperativas de ahorro y crédito del segmento cuatro y las empresas reguladas por la superintendencia de compañías, en este caso se puede analizar que los usuarios por ejemplo si pueden acceder a la información de otros departamentos al no contar con una red segmentada exponiendo así la información crítica para la empresa.

Este control es necesario para las empresas pues viene hacer un proceso que permite agrupar lógicamente activos de red, recursos y aplicaciones, junto a las zonas compartimentadas que no tienen relaciones de confianza entre sí previniendo de esta forma incidentes en la S.I.

16. ¿En caso de contratar soporte técnico externo exige cláusulas de seguridad de confidencialidad en la información?

Tabla 32

Soporte técnico externo - confidencialidad

Opciones	Frecuencia	Porcentaje válido
No	3	11,54%
Si	23	88,46%
Total	26	100,00%

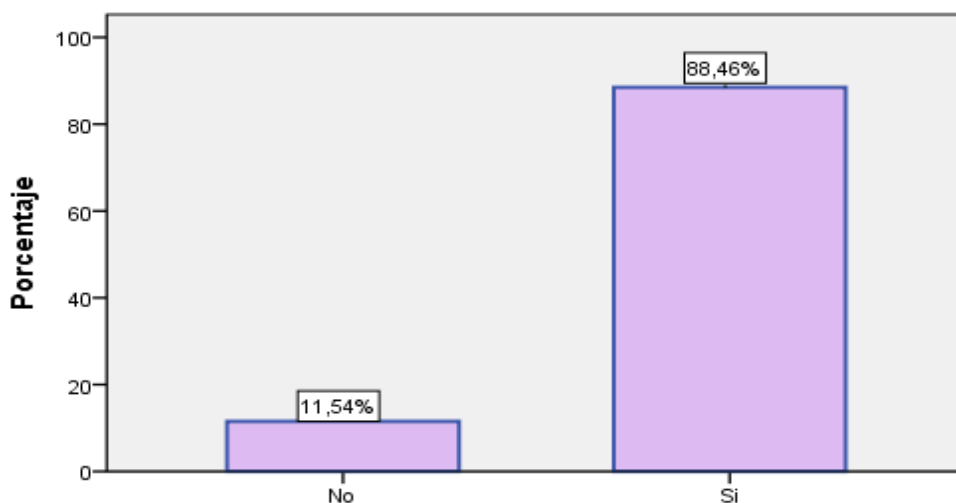


Figura 25. Soporte técnico externo - confidencialidad

Análisis

El 88.46% del total de las empresas encuestadas reguladas por los respectivos organismos de control respondieron que al contratar soporte técnico externo si exigen cláusulas de seguridad de confidencialidad en la información, mientras que el 11,54% no exigen cláusulas de seguridad de confidencialidad en la información al contratar soporte técnico externo, representado a este resultado una entidad del segmento uno y ciertas entidades del segmento cuatro.

17) ¿Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información están debidamente protegidos contra la interceptación, interferencia o posibles daños?

Tabla 33

Protección cables eléctrico y telecomunicaciones

Opciones	Frecuencia	Porcentaje válido
Si	26	100,00%
Total	26	100,00%

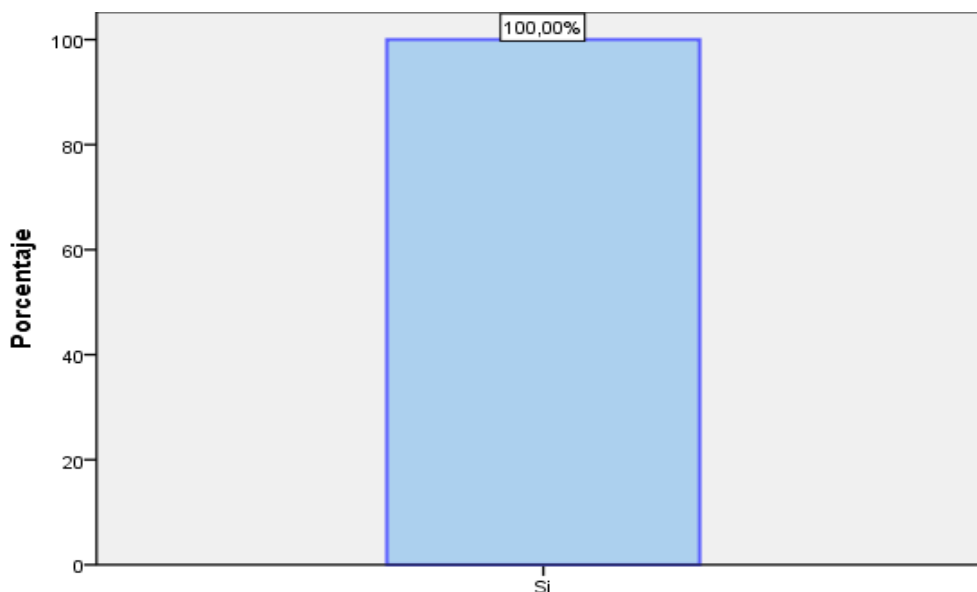


Figura 26. Protección cables eléctricos y telecomunicaciones

Análisis

La totalidad de entidades encuestadas reguladas por los respectivos organismos de control, representando el 100% evidencian que los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información si están debidamente protegidos contra la interceptación, interferencia o posibles daños.

Mediante la observación directa en cada una de las entidades se pudo constatar que los cables eléctricos y de telecomunicaciones están protegidos a través de canaletas proporcionando seguridad del cableado en sí.

18. ¿El software utilizado en los ordenadores cuentan con licencias originales?

Tabla 34

Licencias originales

Opciones	Frecuencia	Porcentaje válido
No	9	34,6
Si	17	65,4
Total	26	100,0

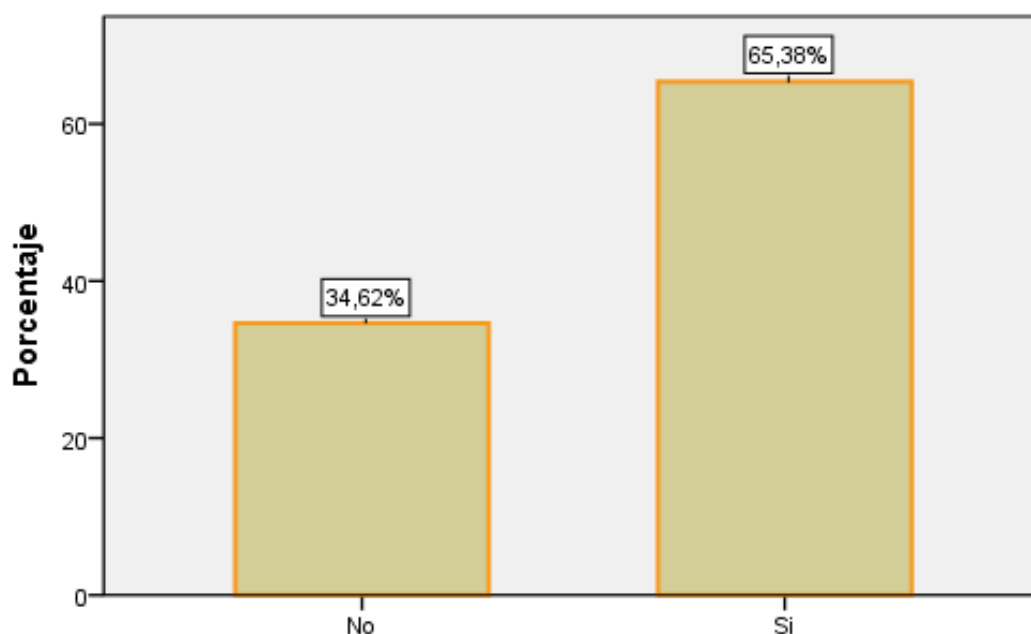


Figura 27. Licencias originales

Análisis

Del total de las entidades encuestadas reguladas por los respectivos organismos de control se evidencia que el 65,38% de las empresas si cuenta con licencias originales de los software's que utilizan en la entidad, mientras que un 34,62% de los encuestados no dispone de licencias originales de los software's que utilizan, dentro de este resultado corresponde a las entidades reguladas por la superintendencia de compañías, seguido por las entidades del segmento cuatro y el resto corresponde a las entidades de los demás segmento.

Al no disponer de licencias originales se correrá grandes riesgos en cuanto a seguridad se refiere ya que puede darse lugar a la pérdida y corrupción de los datos, además al ser un software pirata puede presentar

problemas de compatibilidad y no recibir todas las actualizaciones necesarias para el funcionamiento oportuno y adecuado para ejecutar las labores de la entidad.

19) Los sistemas a ser implantados son inicialmente revisados para detectar códigos maliciosos que afectan a la seguridad de la información.

Tabla 35

Revisión de sistemas a ser implantados

Opciones	Frecuencia	Porcentaje válido
No	6	23,08%
Si	20	76,92%
Total	26	100,00%

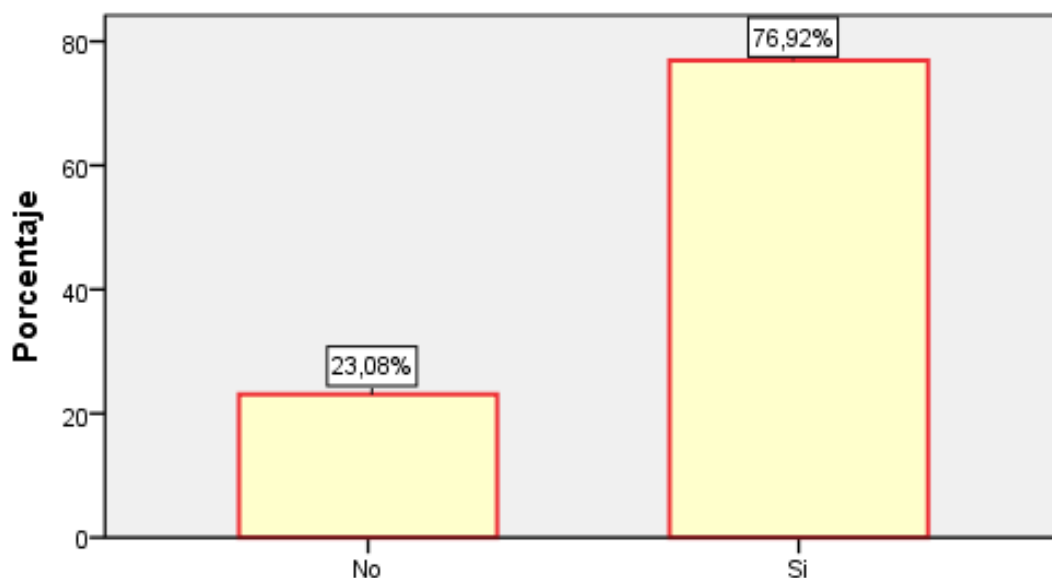


Figura 28. Revisión de sistemas a ser implantados

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control, los resultados obtenidos evidencia que el 76.92% previo a implantar un nuevo sistema estos si son revisados inicialmente para detectar códigos maliciosos que afectan a la seguridad de la información, mientras que el 23.08% manifiesta que no realizan esta actividad misma que se da lugar por no contar con un departamento propio que se encargue de la seguridad de la información ocupándose de la misma un servicio de externalización.

20. ¿Se realiza copias de seguridad de toda la información crítica para la organización?

Tabla 36

Copias de Seguridad

Opciones	Frecuencia	Porcentaje válido
No	4	15,38%
Si	22	84,62%
Total	26	100,00%

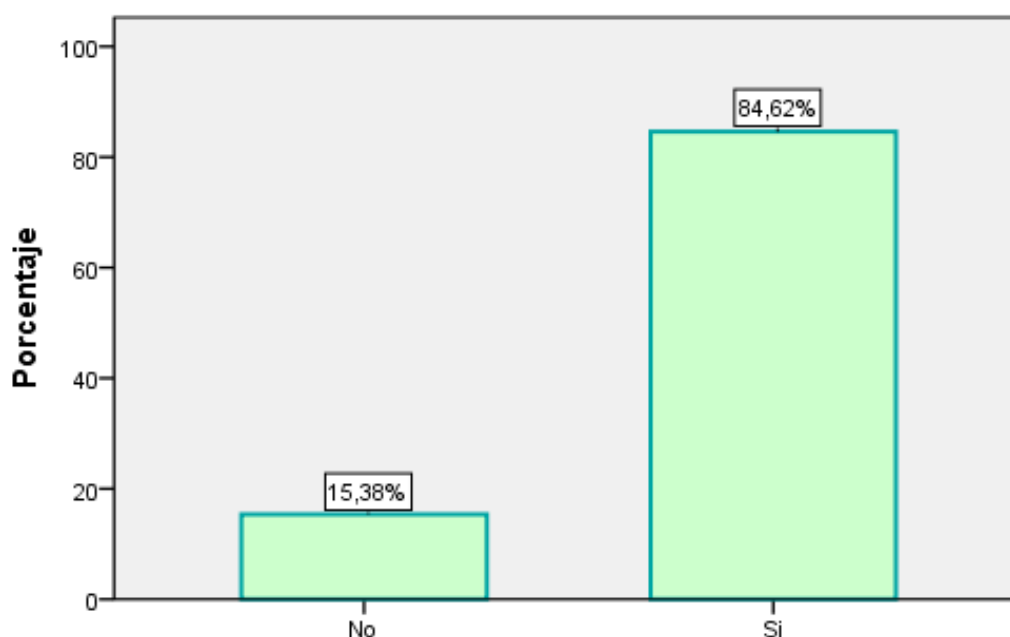


Figura 29. Copias de Seguridad

Análisis

Del resultado obtenido del total de entidades encuestadas reguladas por los respectivos organismos de control, el 84,62% indica que si realizan copias de seguridad de toda la información crítica para la organización, mientras que solo el 15,38% no efectúan las respectivas copias de seguridad en este caso dentro de tal porcentaje abarca a las entidades reguladas por la Superintendencia de Compañías y dos cooperativas de ahorro y crédito del segmento cuatro sin embargo al ser un porcentaje mínimo estas entidades no podrían alcanzar un grado de protección deseado contra la posible pérdida de datos.

20. ¿Se realiza copias de seguridad de toda la información crítica para la organización? ¿Cada que tiempo se realizan copias de seguridad?

Tabla 37

Frecuencia copias de seguridad

Opciones	Frecuencia	Porcentaje válido
Diario	12	46,15%
Semanal	5	19,23%
Mensual	2	7,69%
Trimestral	1	3,85%
Semestral	2	7,69%
No aplica	4	15,38%
Total	26	100,00%

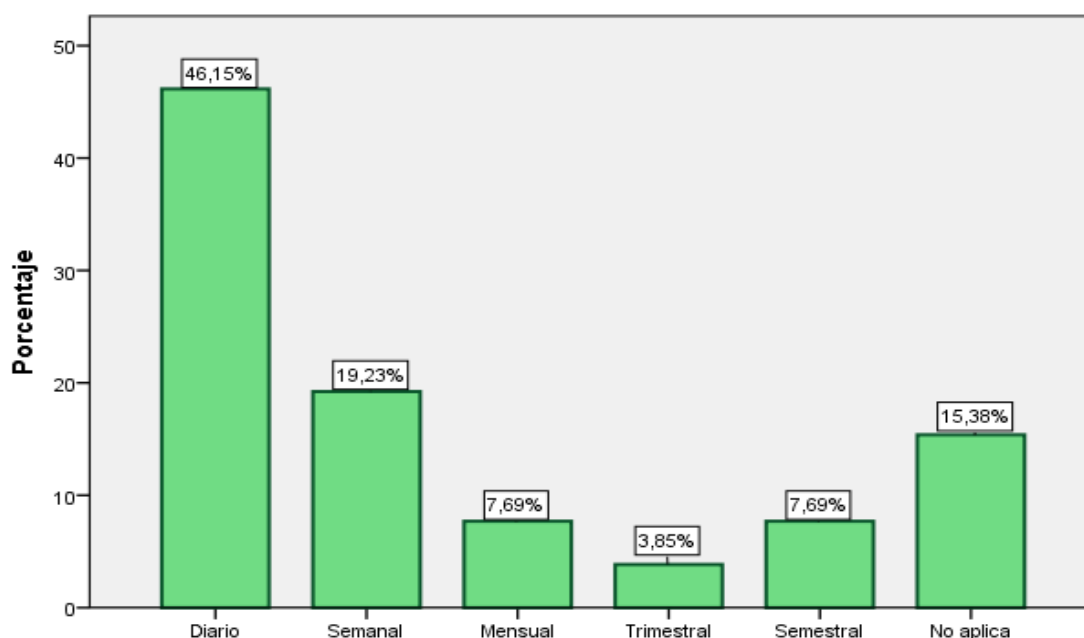


Figura 30. Frecuencia de copias de seguridad

Análisis

De las entidades encuestadas reguladas por los respectivos organismos de control, que realizan copias de seguridad de la información el 46,15% lo efectúa diariamente aquí se encuentran la mayoría de cooperativas de ahorro y crédito correspondientes al segmento dos y tres por otro lado el 19,23% lo realiza de forma semanal, el 7,69% lo hace de forma mensual, el 3,85% realiza las copias trimestralmente y el 7,69% semestralmente.

21) Se posee un gestor de contraseñas, para creación y almacenamiento

Tabla 38

Gestor de contraseñas

Opciones	Frecuencia	Porcentaje válido
No	16	61,54%
Si	10	38,46%
Total	26	100,00%

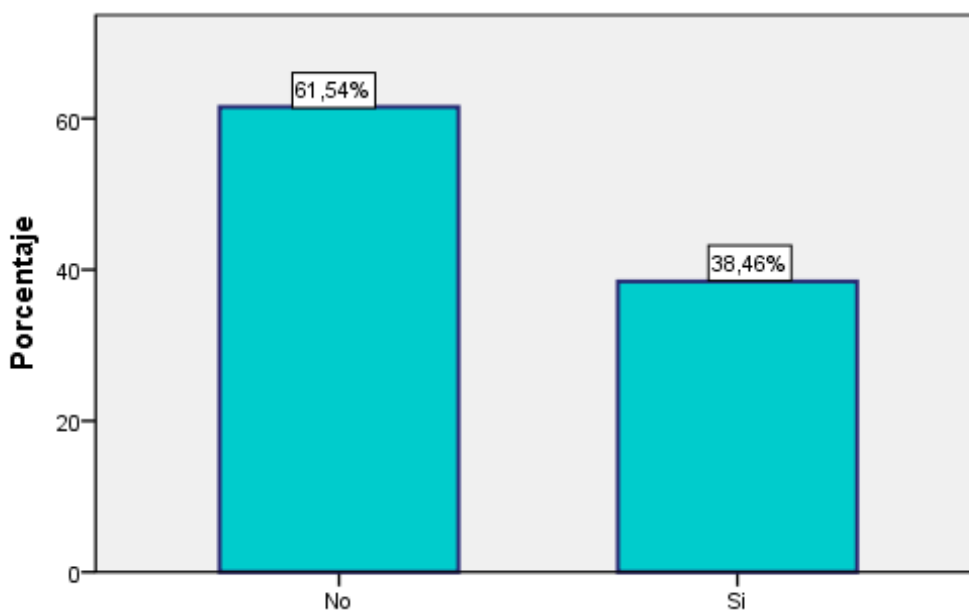


Figura 31. Gestor de contraseñas

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control los resultados evidencian que el 38,46% si posee un posee un gestor de contraseñas, para creación y almacenamiento, mientras que el 61,54% no cuenta con un gestor de contraseñas aquí se ubican la mayoría de entidades de los segmentos tres, y cuatro así también las entidades reguladas por la superintendencia de compañías. Por lo tanto al no contar con esta herramienta existe una gran brecha de inseguridad ya que los sistemas de gestión de contraseñas no serían interactivos ni asegurarían contraseñas de calidad, además estos programas son muy útiles en las empresas ya que guardan múltiples contraseñas y cifran el listado, de tal modo que pueda ser consultado desde allí siempre que se

necesite, para lo cual, solo es necesario recordar una contraseña maestra, que será la responsable de abrir el listado

22) ¿Los ordenadores actualizan automáticamente el sistema operativo?

Tabla 39

Actualización automática ordenadores

Opciones	Frecuencia	Porcentaje válido
No	10	38,46%
Si	16	61,54%
Total	26	100,00%

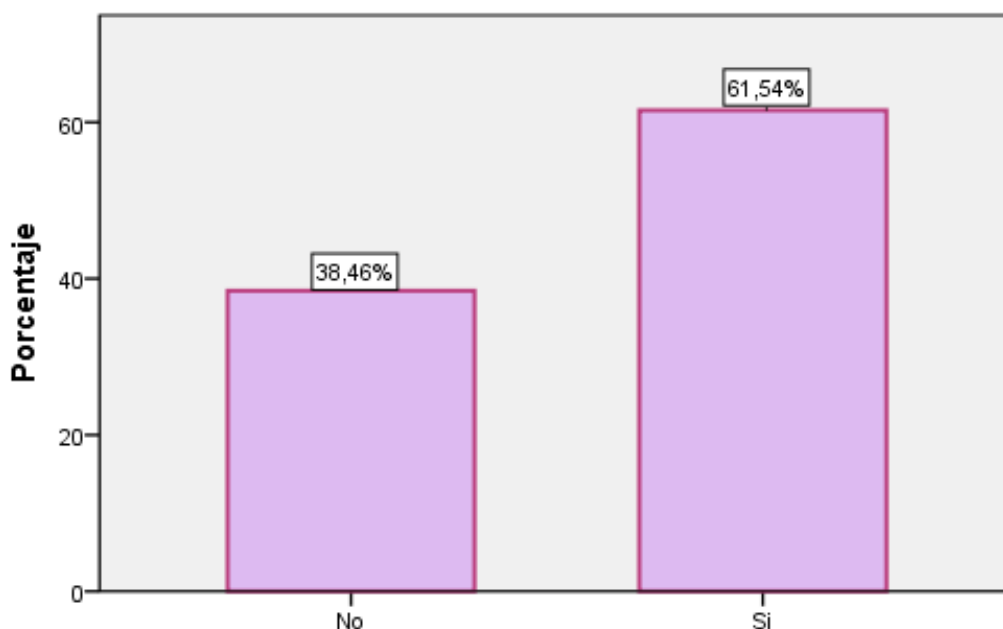


Figura 32. Actualización automática ordenadores

Análisis

Del total de encuestas aplicadas a las entidades del sector servicios reguladas por la SEPS y por la Superintendencia de compañías se evidencia que el 61,54% de los ordenadores que poseen las entidades si actualizan automáticamente el sistema operativo, mientras que el 38,46% no lo hace en este caso es un punto positivo ya que las actualizaciones solo se los debe ejecutar manualmente por el personal autorizado en este caso los departamento encargados de la Seguridad de la información, ya que de esa

forma se observara primero si existe compatibilidad con el Sistema operativo y demás aplicaciones del sistema.

23) ¿Tiene usted restricciones para el uso de internet y sistemas de la empresa?

Tabla 40

Restricciones uso de internet

Opciones	Frecuencia	Porcentaje válido
No	11	42,31%
Si	15	57,69%
Total	26	100,00%

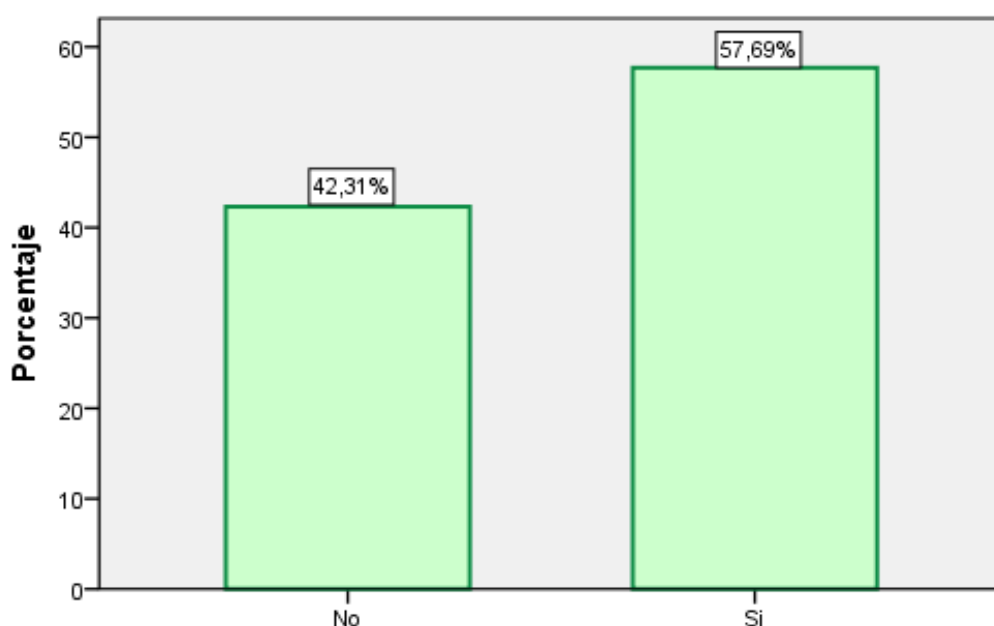


Figura 33. Restricción uso de internet

Análisis

Del total de encuestados regulados por los respectivos organismos de control de los resultados obtenidos se evidencia que un 57,69% de las empresas si tiene restricciones para el uso de internet y sistemas de la empresa, mientras que el 42,31% no tiene restricciones para el uso de internet y sistemas de la empresa, en este caso representa la mayor parte cooperativas de ahorro y crédito del segmento cuatro así también las entidades reguladas por la Superintendencia de Compañías,, sin embargo se puede analizar que es un porcentaje bastante alto de entidades que no consideran este control por lo tanto están expuestos a posibles brechas e incidentes de seguridad de la información.

24) ¿Para áreas seguras, se cuentan con controles de ingreso del personal?

Tabla 41

Áreas seguras

Opciones	Frecuencia	Porcentaje válido
No	11	42,31%
Si	15	57,69%
Total	26	100,00%

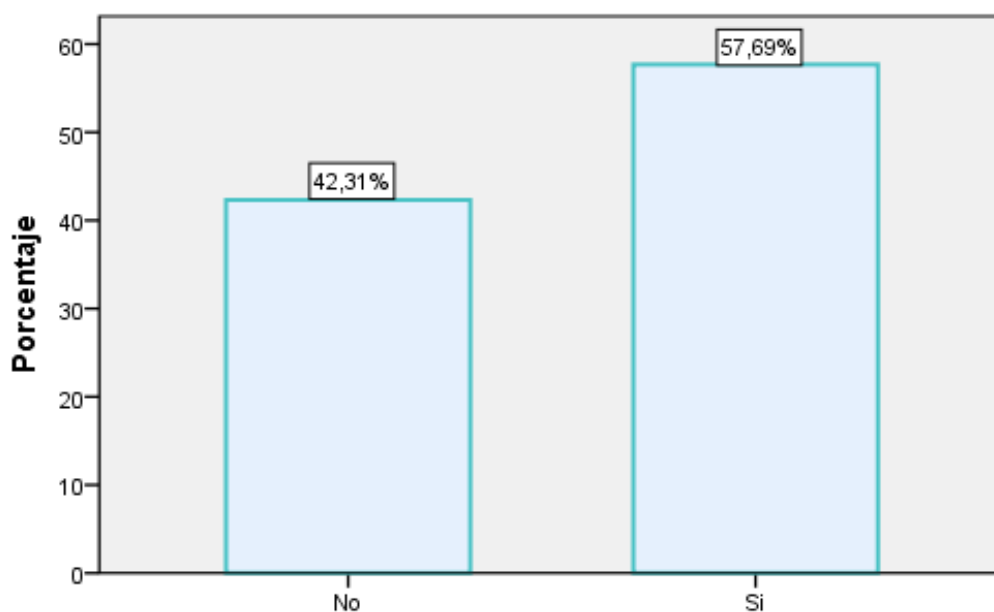


Figura 34. Áreas seguras

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control de los resultados obtenidos se observa que el 57,69% si cuenta con controles de acceso al personal para áreas seguras mientras que el 42,31% de las entidades no aplica controles de acceso al personal para áreas seguras de la empresa.

Las entidades que aplican esta medida evitan el acceso físico no autorizado a las áreas seguras, garantizando que solo el personal autorizado disponga de permiso de acceso aquellas áreas e instalaciones donde se tiene activos de la información sensible y crítica para la empresa.

25) ¿Se comunica eventos de inseguridad y puntos débiles en la seguridad de la información a todo el personal de la entidad?

Tabla 42

Comunicación eventos de inseguridad en la S.I

Opciones	Frecuencia	Porcentaje válido
No	5	19,23%
Si	21	80,77%
Total	26	100,00%

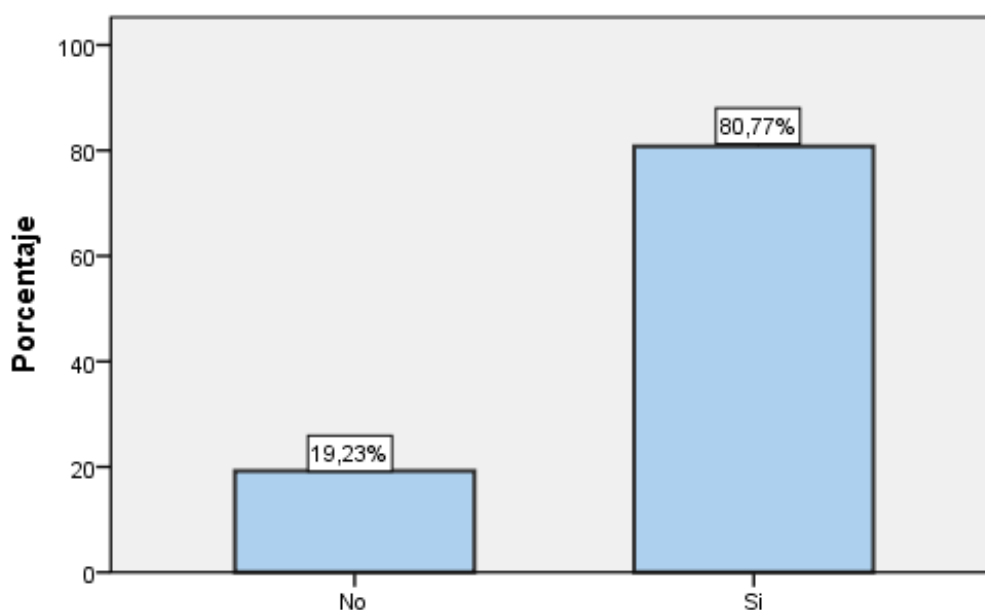


Figura 35. Comunicación eventos de inseguridad en la S.I

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control se puede indicar que el 80,77% si comunica eventos de inseguridad y puntos débiles en la seguridad de la información a todo el personal de la empresa, sin embargo el 19,23% de los encuestados menciona que no comunica los eventos de inseguridad y puntos débiles que se manifiestan en la organización a todo el personal.

Este control se enfoca en la gestión de incidentes el mismo que se basa en la comunicación oportuna de los incidentes solo al personal encargado de solucionar el problema es decir quien está a cargo del departamento de sistema de información, de tal forma es muy importante que todos quienes colaboran en las empresas y utilicen un sistema, al momento de observar

cualquier debilidad sospechosa en la S.I se anote y se informe inmediatamente al personal autorizado de modo que se apliquen acciones correctivas en el tiempo oportuno.

26. ¿La instalación de un software es realizado sólo por el personal autorizado?

Tabla 43

Instalación Software

Opciones	Frecuencia	Porcentaje válido
Si	26	100,00%
Total	26	100,00%

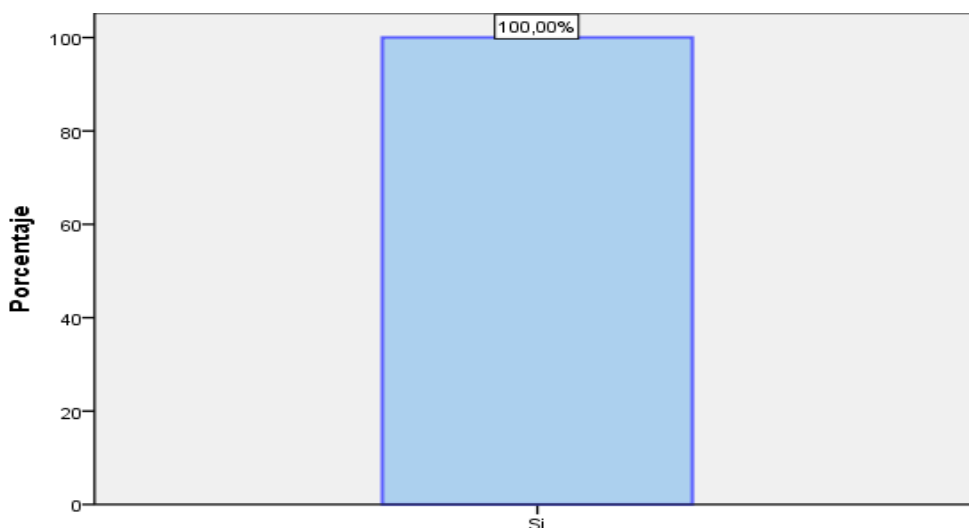


Figura 36. Instalación Software

Análisis

Como resultado de esta pregunta se puede observar que tanto las entidades reguladas por la Superintendencia de Compañías, así como las entidades reguladas por la SEPS, al momento de proceder a la instalación de un software si es realizado sólo por el personal autorizado es decir que el 100% de los encuestados aplican este control de seguridad de manera correcta para evitar que se produzcan incidentes relacionados a la Seguridad de la Información.

27) ¿Recibió usted capacitación en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información?

Tabla 44

Capacitación en S.I

Opciones	Frecuencia	Porcentaje válido
No	12	46,15%
Si	14	53,85%
Total	26	100,00%

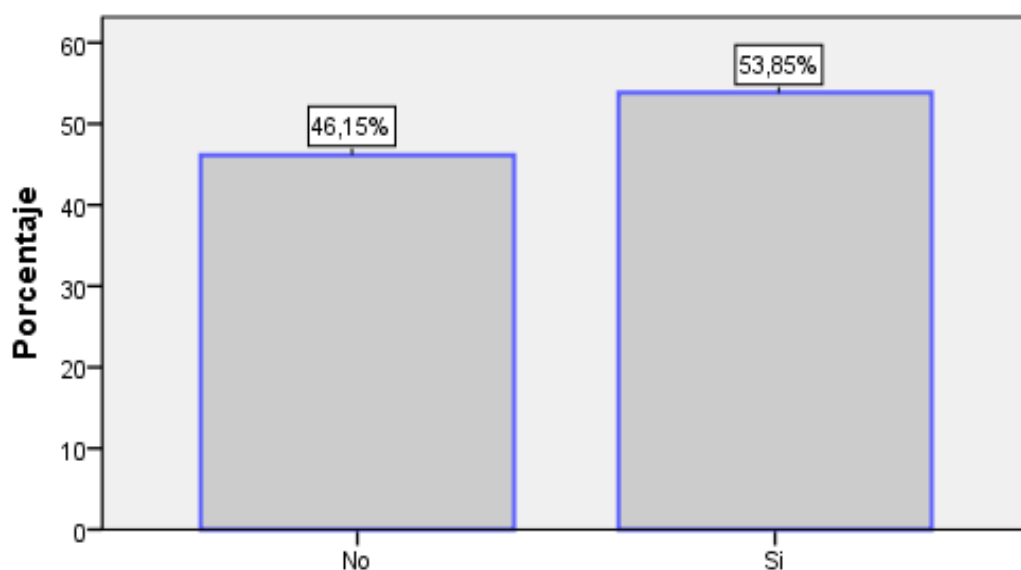


Figura 37. Capacitación en S.I

Análisis

Del total de entidades encuestadas reguladas por los respectivos organismos de control de los resultados obtenidos se puede observar que el 53,85% si recibió capacitación en las empresas sobre procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información, mientras que el 46,15% no recibió ningún tipo de capacitación relacionado a este tema de esta parte de los encuestados se encuentran en su mayor parte las cooperativas de ahorro y crédito del segmento dos y cuatro.

Cabe analizar que existe una brecha bastante estrecha entre los que fueron y no fueron capacitados, en este sentido las entidades deberían considerar aplicar este control ya que todos quienes laboran en la entidad deberían recibir entrenamiento apropiado del conocimiento y actualizaciones

regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

28) ¿En qué ciudad contrata proveedores de servicios en Herramientas de seguridad y protección de Datos?

Tabla 45

Proveedores de Herramientas de S.I

	Latacunga	Ambato	Quito	Cuenca	Guayaquil
Caso Estudio 1	0	0	1	0	1
Caso Estudio 2	0	0	1	0	0
Caso Estudio 3	0	0	1	0	1
Caso Estudio 4	0	0	1	0	0
Caso Estudio 5	0	0	1	0	0
Caso Estudio 6	0	0	1	0	0
Caso Estudio 7	0	1	1	0	0
Caso Estudio 8	0	0	1	0	0
Caso Estudio 9	0	0	0	1	0
Caso Estudio 10	0	0	1	0	0
Caso Estudio 11	0	0	1	1	0
Caso Estudio 12	0	0	1	0	0
Caso Estudio 13	0	0	1	0	0
Caso Estudio 14	0	0	1	0	0
Caso Estudio 15	0	0	1	0	0
Caso Estudio 16	0	0	1	0	0
Caso Estudio 17	0	0	1	0	0
Caso Estudio 18	1	0	0	0	0
Caso Estudio 19	0	0	1	0	0
Caso Estudio 20	0	0	1	0	0
Caso Estudio 21	1	1	1	0	0
Caso Estudio 22	0	0	1	0	0
Caso Estudio 23	1	0	1	0	0
Caso Estudio 24	0	0	1	0	0
Caso Estudio 25	1	0	0	0	0
Caso Estudio 26	0	0	1	0	0
Total empresas	4	2	23	2	2
%	15%	8%	88%	8%	8%

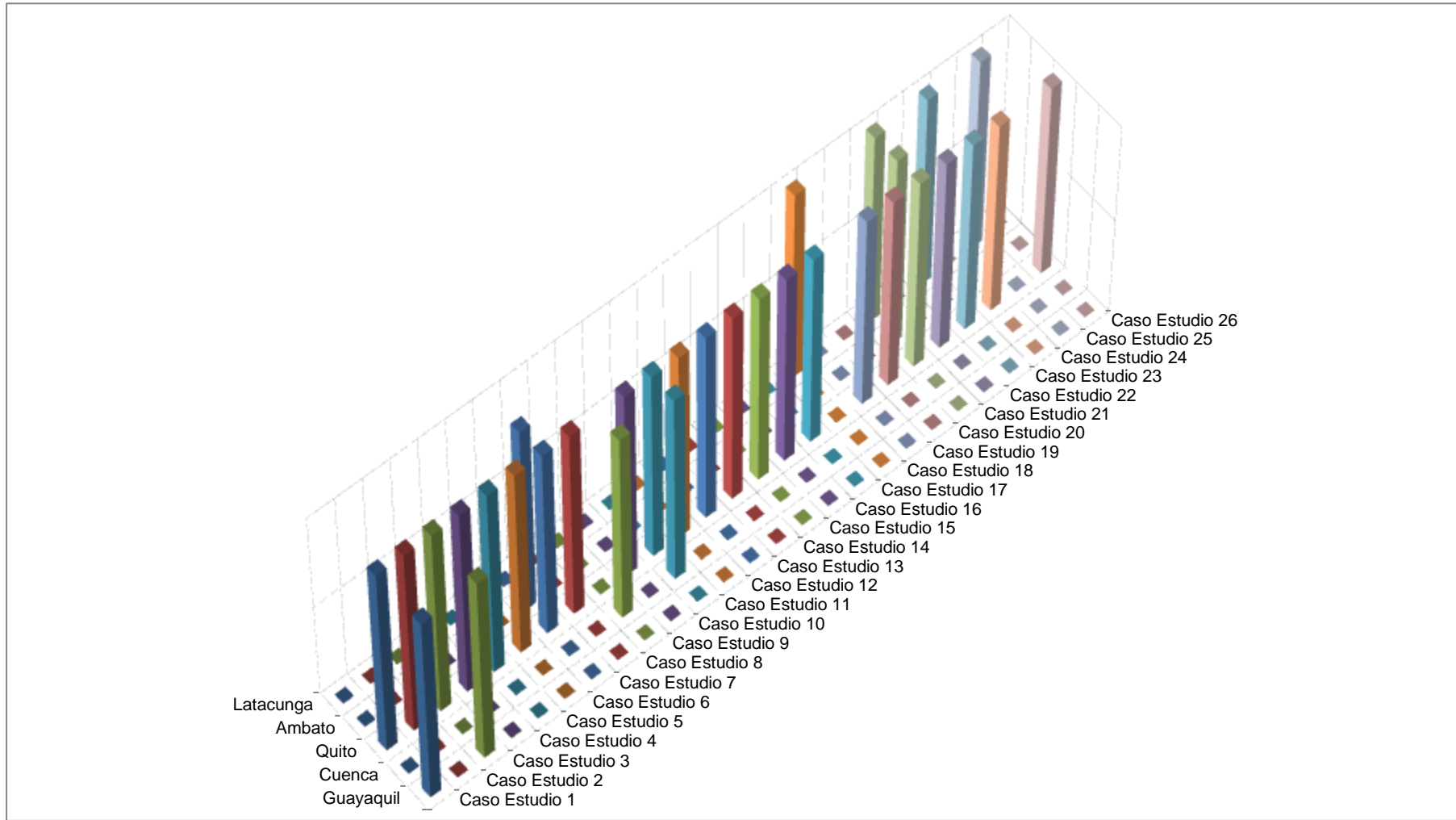


Figura 38. Proveedores de Herramientas de S.I

Análisis

El 88% empresas de servicios trabajan con proveedores de la ciudad de Quito, mientras que el 15% en el cantón Latacunga y el 8% trabajan con proveedores de servicios de herramientas de seguridad y protección de datos de la ciudad de Ambato, Cuenca y Guayaquil.

Basada en la encuesta se establece que en la ciudad de Latacunga no existe una gran oferta en herramientas de seguridad y protección de datos, en su lugar la mayor parte de empresas recurren a ciudades grandes como Quito.

4.4. Comprobación Hipótesis

Para la solución del problema planteado, la comprobación de la hipótesis se establecerá utilizando la prueba estadísticas del Chi X2, misma que se obtendrá a través de la herramienta estadística SPSS.

Hipótesis

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.

Para la verificación de la hipótesis se realizó las siguientes preguntas:

- ¿Cuánto es el monto de inversión, que fue asignado para la seguridad de la información, durante el periodo 2012 al 2016?
- ¿Actualmente se aplica herramientas de Seguridad de la Información en la entidad?

Variables que intervienen

- **Variable dependiente:** Costo-Beneficio para las empresas del sector servicios reguladas por la Superintendencia de Compañías y por la SEPS en sistemas de protección de datos.

- **Variable independiente:** Inversión en la aplicación de herramientas de seguridad de la información

Los resultados obtenidos en la encuesta relacionada con la pregunta utilizada para la comprobación de la hipótesis se demuestran en la siguiente tabla mediante el cruce de variables respectivos obteniendo así la siguiente tabla de contingencia, a través del programa estadístico SPSS:

Tabla 46
Cruce de Variables

		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

Previo al cruce de variables de igual manera, con la herramienta estadística SPSS obtenemos el resultado respecto al cálculo del Chi Cuadrado χ^2 para saber cuál es la decisión con respecto a la hipótesis de la investigación:

Tabla 47

Pruebas del Chi Cuadrado

	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.			

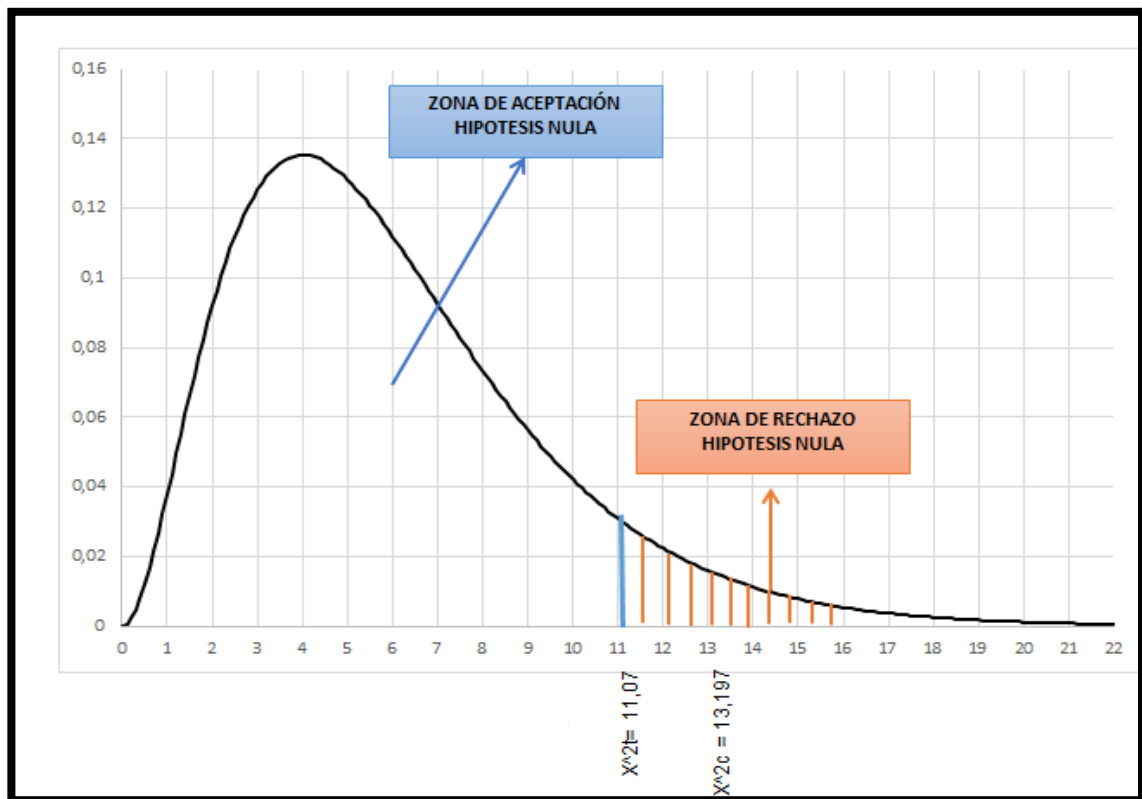
Determinación gráfica del χ^2 crítico

Figura 39. Regla de Decisión

Tomando en cuenta el nivel de significancia del 5% lo cual implica que existe un nivel de confianza del 95%, y analizando el grado de libertad es 5, se toma el valor de 13,197 como valor de referencia para la regla de decisión.

Decisión:

Como $X^2_c=13,197 > X^2_t= 11,07$ se determina zona de rechazo, por lo que se acepta la hipótesis alternativa y se rechaza la H_0 .

Conclusión:

Con un nivel de significancia del 5% que indica una probabilidad de cometer un 0,05 de error tipo I, se encuentra evidencia que 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.

CAPÍTULO V

5. PROPUESTA

5.1. Datos informativos

- **Título:**

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 expuestas las entidades.

- **Entidad Ejecutora**

Empresas del sector servicios Reguladas por la Superintendencia de compañías correspondientes a los ramos de enseñanza, salud, alojamiento, actividades administrativas y de apoyo, adicionalmente se trabajó con entidades Reguladas por la SEPS de los segmentos uno, dos, tres y cuatro.

- **Beneficiarios**

La propuesta beneficia a los directivos, administradores y demás colaboradores de las entidades, puesto que en base a las soluciones expuestas se busca mitigar en cierta medida los riesgos asociados a la Seguridad de la Información y proteger de manera más oportuna los activos de la información.

- **Ubicación**

País: Ecuador

Provincia: Cotopaxi

- **Equipo técnico**

✓ Cofre Santo Tania Stefanía

✓ Remache Soto Victoria Carolina

5.2. Antecedentes de la propuesta

Una vez realizada la investigación y haber determinado que la que 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, además de haber analizado los resultados obtenidos en la encuesta aplicada se logró determinar los incidentes, brechas de seguridad y demás problemas relacionados a los controles de la ISO 27002 de cada uno de los casos de estudio, producidos anualmente dentro del periodo 2012-2016, mismos que han afectado los activos de la información generando costos por tales incidentes.

Por lo tanto se propone la creación de un simulador de inversión para Seguridad de la Información, basado en el diseño de una matriz costo-beneficio, de los incidentes y demás problemas producidos por controles no implementados en las entidades casos de estudio, para lo cual la información se distribuye de acuerdo a cada uno de los segmentos uno, dos, tres y cuatro en lo que tiene que ver con entidades reguladas por la SEPS ya que de esa forma se obtiene un promedio de acuerdo a las características de cada grupo estudiado, así mismo se tomó como otro grupo, solo a las entidades reguladas por la Superintendencia de Compañías.

El simulador permite obtener información en cuanto a un presupuesto estimado que deben asignar específicamente a seguridad de la información las entidades de acuerdo al segmento o sector al que pertenecen, además de conocer también el beneficio marginal a través del indicador ROSI para conocer si la inversión es financieramente viable y cuanto se va a dejar de perder al tener herramientas y medidas que ayuden a mitigar este tipo de riesgos.

5.3. Justificación

La matriz costo- beneficio de las soluciones, políticas propuestas y el simulador de inversión son diseñados con la finalidad de proporcionar información más necesaria correspondiente al presupuesto mínimo que deben

asignar para seguridad de la información, así mismo el simulador es una herramienta complementaria que brinda la facilidad a los directivos y administradores que a pesar de no tener un conocimiento técnico en lo que se refiere a informática podrán basarse o guiarse en cada uno de los puntos establecidos para que a través del ingreso de datos puntuales puedan obtener el beneficio marginal que representará asignar cierto monto en base a las soluciones o controles expuestos que se necesite implementar en la empresa y aminorar los riesgos que se estén suscitando en la entidad.

Con la propuesta planteada lo que se busca también es que la perspectiva gerencial en las empresas cambie, ya que a través de este instrumento de consulta podrán observar que una vez implementado las herramientas y demás medidas para garantizar la ciberseguridad, el presupuesto de inversión para los años siguientes que se debe destinar, no es un monto fuerte que no puedan considerar las entidades, conociendo que dicha inversión realmente les arroja un retorno favorable, además el tema de protección y seguridad de datos en las entidades es algo que siempre debe girar en torno a la mejora continua ya que cada año va evolucionado las formas de ciberdelincuencia por lo que es indispensable contar al menos con las medidas básicas para hacer frente a estos problemas de seguridad de la información.

5.4. Objetivos de la propuesta

5.4.1. Objetivo General

Proporcionar un instrumento que permita determinar los costos y el retorno de la inversión de la seguridad de la información y protección de datos en las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la SEPS.

5.4.2. Objetivos Específicos

- Determinar los controles de la Norma ISO 27002 no implementados por las empresas y los incidentes de seguridad producidos, formulando políticas y

lineamientos para hacer frente a los problemas de seguridad de la información.

- Elaborar una matriz costo-beneficio para evaluar el impacto económico de adquirir una herramienta o mecanismo de protección a los activos de la información.
- Desarrollar un simulador de inversión en Microsoft Excel que posibilite el cálculo de los costos y el beneficio marginal en seguridad de la información, convirtiéndose para la administración de las empresas un instrumento de apoyo en el momento de tomar decisiones.

5.5. Diseño de la propuesta

El análisis se realizó por segmentos uno, dos, tres y cuatro de entidades reguladas por la SEPS, y de las empresas reguladas por la Superintendencia de Compañías se efectuó un estudio en conjunto entre las entidades dedicadas a las actividades administrativas de apoyo, enseñanza, salud y alojamiento.

Inicialmente se determinó los controles que según la Norma ISO27002 no han sido aplicadas en las organizaciones, así también es necesario conocer los incidentes de seguridad producidos, una vez obtenida la información es momento de formular políticas y lineamientos que sirven como marco de referencia para el manejo y operatividad de los sistemas de información.

Posteriormente se mostrará una matriz costo - beneficio, para evaluar si en un momento determinado en el tiempo, el costo de una medida específica es mayor que los beneficios resultantes de la misma, además permite estimar cuál opción de herramienta o mecanismo de seguridad para la información es más adecuada en términos económicos.

Finalmente la propuesta para la presente investigación consiste en el diseño de un simulador de inversión que muestra resultados económicos que puede llegar a suceder, convirtiéndose en un instrumento de apoyo para la administración de las empresas del sector servicios a la hora de tomar decisiones de inversión en seguridad de la información.

A continuación se presenta una tabla de las principales fases para el desarrollo de la propuesta.

Tabla 48

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.	<p>Detallar las principales debilidades detectadas por grupo de empresas luego de aplicar los distintos métodos de análisis y recolección de información.</p> <p>Formular políticas y lineamientos de seguridad que son una parte importante para el éxito de la operatividad en las empresas.</p>
FASE II	Elaborar una matriz costo-beneficio para evaluar el impacto económico de adquirir una herramienta para proteger los activos de la información.	<p>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.</p> <p>Se enuncia los costos de inversión conseguidos a través de empresas proveedoras de herramientas de seguridad.</p> <p>Se determina el beneficio marginal luego de aplicar el cálculo del indicador ROSI.</p>
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	<p>Instrucciones para usar correctamente el simulador.</p> <p>Plantilla de datos.</p> <p>Usar fórmulas y funciones del Excel.</p> <p>Ejecución del simulador de inversión.</p>

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

CONTINUA 

COSTO/BENEFICIO DE INVERTIR EN PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN

EMPRESAS DEL
SECTOR SERVICIOS

ORGANISMOS
REGULADORES



Previo a la investigación realizada se ha evidenciado ciertas debilidades en cada uno de los casos estudiados, en relación a la inversión en herramientas de seguridad y protección de datos, por esta razón se ha visto conveniente brindar una solución frente a los incidentes y demás problemas de seguridad de la información con la aplicación de controles en base a la normativa ISO/IEC 27002, y a su vez el costo que representa proteger la seguridad de la información, en su conjunto esto permitirá conocer un presupuesto aproximado, que necesariamente las entidades deberán destinar a la inversión en Seguridad de la Información.

Nota: El texto subrayado de este color son los problemas de seguridad de la información, más comunes detectadas en cada segmento o tipo de empresa.

2012-2016



PROBLEMAS DE SEGURIDAD DE LA INFORMACIÓN

1. Ausencia de políticas de uso de controles criptográficos
2. Ausencia de política de seguridad de la Información para proveedores.
3. Actualización automática del sistema operativo.
4. Se comunica las fallas de S.I a todo el personal.
5. Ataque o infección por código malicioso.
6. Ingeniería social, fraude o phishing

(Información tomada de las encuestas)

POLÍTICAS DE SEGURIDAD PARA PROTEGER LA INFORMACIÓN

Políticas

1. Asegurar la integridad y la confidencialidad de la información que maneja la entidad.
2. Todo proveedor de la entidad podrá desarrollar para la empresa aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios, acatando con responsabilidad cada uno de los acuerdos, lineamientos y normativas que imponga la empresa.
3. Las nuevas implementaciones o actualizaciones de software debe estar sujetas a revisión.
4. Todo comunicado que se efectúe en la entidad debe ser transmitido únicamente al personal correspondiente.

Lineamientos

1. 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.
2. Realizar la formalización de un acuerdo escrito de confidencialidad debidamente firmado entre las partes antes de efectuar las actividades técnicas contratadas a empresas externas de modo que la información no podrá ser utilizada en ningún caso fuera del marco establecido.
3. Toda actualización del sistema operativo debe ser revisada su compatibilidad con los programas que utiliza la empresa para su posterior instalación en los equipos.
4. 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.

SOLUCIÓN /COSTOS – PARA LA TOTALIDAD DE PROBLEMAS

SOLUCIÓN	Costo
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Configuración Red inalámbrica y red local	\$ 200,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Concienciación, educación y capacitación en S.I	
Charla sobre Ingeniería social, fraude o phishing, un día.	\$ 200,00
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Firewall Empresarial + compra de equipo	\$ 3.000,00
Licencia Anual Firewall	\$ 5.000,00

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



SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

SEGMENTO 1

**ACTIVOS MAYORES A
\$80'000.000**

Con el fin de proporcionar una guía y apoyo a la dirección en temas de seguridad de la información, a continuación a modo orientativo se presenta la solución frente a los problemas detectados de acuerdo a los casos de estudio analizados.

SOLUCIÓN	COSTO
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Configuración Red inalámbrica y red local	\$ 200,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Concienciación, educación y capacitación en S.I	
Charla sobre Ingeniería social, fraude o phishing, un día.	\$ 200,00
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Firewall Empresarial + compra de equipo	\$ 3.000,00
Licencia Anual Firewall	\$ 5.000,00
Total Presupuesto de Inversión	\$ 9.030,00

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

En base a los incidentes y los controles de seguridad de la información no aplicados mayormente en las entidades del segmento uno, el presupuesto mínimo estimado para la empresa que por primera vez busca implementar y ejecutar medidas para la seguridad de la información, el monto aproximado de presupuesto para el año uno es de \$ 9.030,00 dólares.

PRESUPUESTO ANUAL ESTIMADO (Para años siguientes)

SOLUCIÓN	COSTO
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Concienciación, educación y capacitación en S.I	
Charla sobre Ingeniería social, fraude o phishing, un día.	\$ 200,00
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Licencia Anual Firewall	\$ 5.000,00
Total Presupuesto de Inversión	\$ 5.730,00

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

Las entidades del segmento 1, una vez que hayan implementado y ejecutado las soluciones más pertinentes para los problemas expuestos, necesariamente el presupuesto anual estimado que se debe asignar es un monto de \$5.730,00 para llevar a cabo las medidas de seguridad de la información.



SEGMENTO 1

ACTIVOS MAYORES A
\$80'000.000

SEGMENTO 2

**ACTIVOS MAYORES A
20'000.000,00 hasta
80'000.000,00**

Con el fin de proporcionar una guía y apoyo a la dirección en temas de seguridad de la información, a continuación a modo orientativo se presenta la solución frente a los problemas más comunes detectados en entidades del segmento dos.

PROBLEMAS DE SEGURIDAD DE LA INFORMACIÓN

1. No existe controles criptográficos
2. No reciben capacitaciones en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información
3. Se comunica las fallas de S.I a todo el personal.
4. Ataque o infección por código malicioso.
5. Ingeniería social, fraude o phishing
6. Uso indebido de información critica
7. No tienen un método o programa para borrar la información confidencial
8. Software sin licencias originales
9. No cuentan con un gestor de contraseñas

131

(Información tomada de las encuestas)

POLÍTICAS DE SEGURIDAD PARA PROTEGER LA INFROMACIÓN

Políticas

Lineamientos

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. Asegurar la integridad y la confidencialidad de la información que maneja la entidad. 2. Se deben definir y coordinar planes de capacitación para el personal que labora en la entidad de modo que se eleven los niveles de sensibilización frente a la protección de la información. 3. Todo comunicado que se efectúe en la entidad debe ser trasmitido únicamente al personal correspondiente. 4. Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque general que involucre controles físicos técnicos, humanos y administrativos | <ol style="list-style-type: none"> 1. 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. 2. Los planes de capacitación, entrenamiento y sensibilización en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información serán llevados a cabo anualmente. 3. 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. 4. Para garantizar la seguridad de la información crítica de la entidad se adquirirá software's con licencias originales, gestores de contraseñas, y 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. |
|---|--|

SOLUCIÓN	COSTO
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, un día.	\$ 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 cada maquina	\$ 40,00
Eliminación de Soportes	
Método o programa para el borrado de información confidencial	\$ 24,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina	\$ 70,00
Paquete Office por máquina	\$ 90,00
Gestión de contraseñas de usuario	
Gestor de contraseñas manual	\$ 20,00

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

PRESUPUESTO ESTIMADO IMPLEMENTACIÓN –De problemas más comunes del segmento

SOLUCIÓN	COSTO
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	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal 25 maquina	\$ 1.000,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina 25 máquinas	\$ 1.750,00
Licencia Paquete Office por máquina 25 máquinas	\$ 2.250,00
Total Presupuesto de Inversión	\$ 5.730,00

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

En base a los incidentes y los controles de seguridad de la información no aplicados mayormente en las entidades del segmento dos, el presupuesto estimado para la empresa que por primera vez busca implementar y ejecutar medidas para la seguridad de la información, el monto aproximado de presupuesto para el año uno es de \$ 5.730,00 dólares.

PRESUPUESTO ANUAL ESTIMADO (Para años siguientes)

SOLUCIÓN	COSTO
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal 25 maquina	\$ 1.000,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina 25 máquinas	\$ 1.750,00
Licencia Paquete Office por máquina 25 máquinas	\$ 2.250,00
Total Presupuesto de Inversión	\$ 5.530,00

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

Como presupuesto anual estimado se obtienen un monto de \$5.530,00 que deben asignar obligatoriamente las entidades del segmento uno para llevar a cabo las medidas de seguridad de la información.



SEGMENTO 2

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



SEGMENTO 3

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

Con el fin de proporcionar una guía y apoyo a la dirección en temas de seguridad de la información, a continuación a modo orientativo se presenta la solución frente a los problemas más comunes detectados en las entidades del segmento tres.

1. Ausencia de políticas de uso de controles criptográficos
 2. Ausencia de política de seguridad de la Información para proveedores.
 3. Ausencia de políticas de intercambio de información
 4. Ausencia de Políticas de puesto de trabajo despejado y bloqueo de pantalla automático.
 5. No reciben capacitaciones en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información
 6. Actualización automática del sistema operativo
 7. Se comunica las fallas de S.I a todo el personal
 8. Software sin licencias originales
 9. No cuentan con un gestor de contraseñas
 10. No tienen un método o programa para borrar la información
 11. Áreas seguras sin control de ingreso
 12. Ataque o infección por código malicioso.
 13. Destrucción no autorizada e la información.
 14. Robo de equipos
 15. Uso indebido de información crítica
 16. Interrupción prolongada en un sistema o servicio de red
 17. Modificación o eliminación no autorizada de datos
 18. Administración y control de red/ Ingreso al sistema de otras áreas
- (Información tomada de las encuestas)

POLÍTICAS DE SEGURIDAD PARA PROTEGER LA INFROMACIÓN

Políticas

Lineamientos

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. Asegurar la integridad y la confidencialidad de la información que maneja la entidad. 2. Todo proveedor de la entidad podrá desarrollar para la empresa aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios, acatando con responsabilidad cada uno de los acuerdos, lineamientos y normativas que imponga la empresa. 3. Toda información que viaja a través del uso de todo tipo de instalaciones de comunicación debe ser manejado con cautela según los acuerdos de intercambio y cumplir con la legislación correspondiente. | <ol style="list-style-type: none"> 1. 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. 2. Realizar la formalización de un acuerdo escrito de confidencialidad debidamente firmado entre las partes antes de efectuar las actividades técnicas contratadas a empresas externas de modo que la información no podrá ser utilizada en ningún caso fuera del marco establecido. 3. Cada persona en la entidad será responsable de la información que está bajo su custodia. |
|---|--|

Políticas

4. La información que maneja el personal debe ser protegida en cualquiera de sus formas una vez que el usuario abandone su puesto de trabajo.
5. Se deben definir y coordinar planes de capacitación para el personal que labora en la entidad de modo que se eleven los niveles de sensibilización frente a la protección de la información.
6. Las nuevas implementaciones o actualizaciones de software debe estar sujetas a revisión.
7. Todo comunicado que se efectúe en la entidad debe ser transmitido únicamente al personal correspondiente.
8. Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque general que involucre controles físicos técnicos, humanos y administrativos
9. Todas las áreas destinadas al procesamiento de la información o de almacenamiento, deben contar con protecciones físicas o perímetros de seguridad, cubriendo controles de entradas físicos, seguridad de oficinas, de manera que solo el personal autorizado dispone de permiso s de acceso.

Lineamientos

4. Cada vez que el usuario se ausente de su puesto de trabajo, se debe activar el protector de pantalla definido y a su vez debe guardar en un lugar seguro cualquier documento y medios que contengan información confidencial y de uso interno.
5. Los planes de capacitación, entrenamiento y sensibilización en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información serán llevados a cabo anualmente .
6. Toda actualización del sistema operativo debe ser revisada su compatibilidad con los programas que utiliza la empresa para su posterior instalación en los equipos.
7. 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.
8. Para garantizar la seguridad de la información crítica de la entidad se adquirirá software's con licencias originales, gestores de contraseñas, y 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.
9. Para evitar intrusión física de personas no autorizadas a áreas seguras se utilizará tecnologías de autenticación, monitoreo y registro de entradas y salidas.



SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

SEGMENTO 3

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

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 el uso indebido de la información crítica	\$ 200,00
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Equipo informático de usuario desatendido	
Configuraciones	\$ 100,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina	\$ 70,00
Licencia Paquete Office por máquina	\$ 90,00
Gestión de contraseñas de usuario	
Gestor de contraseñas manual	\$ 20,00
Gestor de contraseñas por dominios	
Servidor	\$ 3.000
Configuración	\$ 1.500
Eliminación de Soportes	
Método o programa para el borrado de información confidencial	\$ 24,00
Controles físicos de entrada	
Lector biométrico	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por cada maquina	\$ 40,00
Procedimientos seguros de inicio de sesión	
Roles, logs, Integridad por cifrado – Servidor de Dominios	\$3.000,00
Responsabilidades de gestión	
8 Cámaras de seguridad	\$ 800,00
Segregación de redes	
Router	\$ 500,00
Switch	\$ 200,00
Rack	\$ 400,00
Patch Panel	\$ 80,00
Configuraciones	\$1.000,00

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

PRESUPUESTO ESTIMADO IMPLEMENTACIÓN –De problemas más comunes del segmento

SOLUCIÓN	COSTOS
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Configuración Red inalámbrica y red local	\$ 200,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal 15 por máquina	\$ 600,00
Responsabilidades de gestión	
8 Cámaras de seguridad	\$ 800,00
Gestión de contraseñas de usuario	
Gestor de contraseñas	\$ 20,00
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Charla sobre el uso indebido de la información crítica	\$ 200,00
Procedimientos seguros de inicio de sesión	
Roles, logs, Integridad por cifrado	\$ 3.000,00
Total Presupuesto de Inversión	\$ 5.350,00

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

En base a los incidentes y los controles de seguridad de la información no aplicados mayormente en las entidades del segmento tres, el presupuesto estimado para la empresa que por primera vez busca implementar y ejecutar medidas para la seguridad de la información, el monto aproximado de presupuesto para el año uno es de \$ 5.350,00 dólares.



SEGMENTO 3

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

PRESUPUESTO ANUAL ESTIMADO (Para años siguientes)

136

SOLUCIÓN	COSTOS
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal 15 por máquina	\$ 600,00
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Charla sobre el uso indebido de la información crítica	\$ 200,00
Total Presupuesto de Inversión	\$ 1.330,00

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

Como presupuesto anual estimado se obtienen un monto de \$1.330,00 que deben asignar obligatoriamente las entidades del segmento uno para llevar a cabo las medidas de seguridad de la información.



SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

SEGMENTO 3

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



SEGMENTO 4

**ACTIVOS MAYORES A
1'000.000,00 HASTA
5'000.000.00**

Con el fin de proporcionar una guía y apoyo a la dirección en temas de seguridad de la información, a continuación a modo orientativo se presenta la solución frente a los problemas más comunes detectados en las entidades del segmento Cuatro.

1. Ausencia de políticas de control de acceso y autenticación.
2. Ausencia de políticas de uso de controles criptográficos.
3. Ausencia de políticas de intercambio de información.
4. Ausencia de políticas de puesto de trabajo despejado y bloqueo de pantalla automático.
5. Ausencia de políticas de seguridad de la información para proveedores.
6. No reciben capacitaciones en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información.
7. Se comunica las fallas de S.I. a todo el personal
8. No se da de baja a los accesos de los empleados una vez que termine el contrato laboral.
9. Los acuerdos de confidencialidad se firman después de iniciar las labores o incluso no se firman este tipo de acuerdos.
10. Los sistemas a ser implementados no son revisados inicialmente.
11. Ataque o infección por código malicioso.
12. Interrupción prolongada en un sistema o servicio de red.
13. Intento de acceso a un sistema informático.
14. Ingeniería social, fraude o phishing
15. Destrucción no autorizada de la información.
16. Uso indebido de información crítica
17. No se cuenta con un inventario de activos de la información
18. No tienen un método o programa para borrar la información confidencial
19. No se dispone de un registro de los intentos de accesos fallidos y exitosos del sistema.
20. Administración y control de red / ingreso al sistema de otras áreas
21. Software sin licencias originales.
22. No se realizan copias de seguridad de toda la información sensible de la empresa.
23. No cuentan con un gestor de contraseñas
24. Actualización automática del sistema operativo.
25. No tienen restricciones en el uso de internet.
26. Áreas seguras sin control de acceso.

(Información tomada de las encuestas)

POLÍTICAS DE SEGURIDAD PARA PROTEGER LA INFORMACIÓN

Políticas

1. El personal tendrá acceso a los sistemas y demás instalaciones para los que específicamente se les haya autorizado su uso desde la gerencia de la Cooperativa.
2. Asegurar la integridad y la confidencialidad de la información que maneja la entidad.

Lineamientos

1. Necesariamente los empleados de la institución deberán contar con una identificación única personal para acceder a los sistemas y demás instalaciones, relacionadas exclusivamente con las actividades y funciones que debe desempeñar el empleado.
2. 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.

SEGMENTO 4

**ACTIVOS MAYORES A
1'000.000,00 HASTA
5'000.000,00**

Políticas

3. Toda información que viaja a través del uso de todo tipo de instalaciones de comunicación debe ser manejada con cautela según los acuerdos de intercambio y cumplir con la legislación correspondiente.
4. La información que maneja el personal debe ser protegida en cualquiera de sus formas una vez que el usuario abandone su puesto de trabajo.
5. Todo proveedor de la entidad podrá desarrollar para la empresa aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios, acatando con responsabilidad cada uno de los acuerdos, lineamientos y normativas que imponga la empresa.
6. Se deben definir y coordinar planes de capacitación para el personal que labora en la entidad de modo que se eleven los niveles de sensibilización frente a la protección de la información.
7. Todo comunicado que se efectuó en la entidad debe ser transmitido únicamente al personal correspondiente.
8. Una vez confirmado que han cesado las funciones del empleado se debe dar de baja al usuario en el acceso a los sistemas de información.
9. Preparar un respaldo legal para proteger la información que se utiliza por los empleados durante las actividades laborales.

Lineamientos

3. Para proteger la información en los intercambios entre organizaciones se debe resaltar el grado de criticidad de la información y demás especificaciones de seguridad. Además de que cada persona en la entidad será responsable de la información que está bajo su custodia.
4. Cada vez que el usuario se ausente de su puesto de trabajo, se debe activar el protector de pantalla definido y a su vez debe guardar en un lugar seguro cualquier documento y medios que contengan información confidencial y de uso interno.
5. Realizar la formalización de un acuerdo escrito de confidencialidad debidamente firmado entre las partes antes de efectuar las actividades técnicas contratadas a empresas externas de modo que la información no podrá ser utilizada en ningún caso fuera del marco establecido.
6. Los planes de capacitación, entrenamiento y sensibilización en procedimientos de seguridad de la información y el uso correcto de los medios disponibles para el procesamiento de la información serán llevados a cabo anualmente.
7. 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.
8. Para ello se le debe retirar inmediatamente el computador, el teléfono, la tarjeta de acceso, y deshabilitar el usuario y contraseña de la cuenta del sistema de información que utilizaba en el tiempo de labores.
9. Presentar acuerdos escritos de confidencialidad en donde el empleado se comprometa a no revelar a personas ajenas a la empresa la información que maneja.

Políticas**Lineamientos**

- | | |
|--|---|
| <p>10. Para garantizar la calidad del equipo o software adquirido, el personal encargado del área de Seguridad de la Información revisará inicialmente el producto antes de su implementación, en caso de no contar con un experto propio de la empresa, se podrá recurrir a los servicios externos.</p> | <p>10. Verificar que tanto el equipo, así como también el software cumplan con los estándares adecuados y que ejecuten las funciones previstas. Además necesariamente se deberá comprobar de que el software mantenga las medidas de seguridad que permitan detectar códigos maliciosos, virus informáticos y demás que pueden provocar la pérdida de la información.</p> |
| <p>11. Realizar un registro documental ordenado y valorada de los elementos que comprenden los activos de la información</p> | <p>11. Para realizar un inventario de activos de información se puede iniciar clasificando en activos de información pura, activos físicos y activos humanos.</p> |
| <p>12. Eliminación o destrucción segura de la información confidencial de la empresa.</p> | <p>12. 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.</p> |
| <p>13. Mantener procesos de auditoria basada en la revisión de logs que muestran las actividades realizadas por el usuario sobre un sistema, con el objetivo de asegurar el funcionamiento operacional de la seguridad en un sistema.</p> | <p>13. Mantener un registro de intento de accesos fallidos al iniciar sesión, así también registrar los usuarios que no ingresaron la contraseña correcta después algunos intentos, bloquear el ID de usuario en caso de que sobrepase tres intentos de acceso.</p> |
| <p>14. 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.</p> | <p>14. 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.</p> |
| <p>15. El usuario del sistema podrá acceder a los permisos que un desarrollador otorga sobre el sistema</p> | <p>15. Firmar un contrato entre el titular con derechos de la propiedad intelectual y el usuario, por lo que previamente los programas serán valorados.</p> |

**SEGMENTO 4**

**ACTIVOS MAYORES A
1'000.000,00 HASTA
5'000.000,00**

SEGMENTO 4

**ACTIVOS MAYORES A
1'000.000,00 HASTA
5'000.000,00**

Políticas

16. Para asegurar la integridad y disponibilidad de la información se requiere periódicamente aplicar sistemas de Backup.
17. Las nuevas implementaciones o actualizaciones de software debe estar sujetas a revisión.
18. Controlar a los usuarios el acceso a los servicios de internet
19. Permitir el acceso a un área solo al personal autorizado.

Lineamientos

16. Cuando se va a realizar copias de seguridad de la información se debe identificar el tipo de copias y la periodicidad de las mismas, así como los soportes en las que se deben realizar y las ubicaciones de los centros de respaldo.
17. Toda actualización del sistema operativo debe ser revisada su compatibilidad con los programas que utiliza la empresa para su posterior instalación en los equipos.
18. Determinar las direcciones a las cuales el usuario puede ingresar.
19. Para las áreas protegidas se deberá proporcionar a los empleados controles de acceso físico, de tal modo se permita el acceso solo al personal autorizado.

140

SOLUCIÓN /COSTOS – PARA LA TOTALIDAD DE PROBLEMAS

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

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

CONTINÚA



SEGMENTO 4

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

SOLUCIÓN	COSTOS
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

141

PRESUPUESTO ESTIMADO IMPLEMENTACIÓN —De problemas más comunes del segmento

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	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 máquina	\$ 400,00
Eliminación de Soportes	
Método o programa para el borrado de información confidencial	\$ 24,00
Segregación de redes	
Router	\$ 500,00
Switch	\$ 200,00
Rack	\$ 400,00
Patch Panel	\$ 80,00
Configuraciones	\$1.000,00
Gestión de contraseñas de usuario	
Gestor de contraseñas manual	\$ 20,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Controles físicos de entrada	
Lector biométrico	\$ 400,00
Total Presupuesto estimado implementación	\$ 3.854,00

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

En base a los incidentes y los controles de seguridad de la información no aplicados mayormente en las entidades del segmento 4, el presupuesto estimado para la empresa que por primera vez busca implementar medidas para la seguridad de la información, el monto aproximado de presupuesto para el año 1 es de 3.854,00 dólares.

PRESUPUESTO ANUAL ESTIMADO (Para años siguientes)

SOLUCIÓN	COSTOS
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 máquinas	\$ 400,00
Total Presupuesto anual estimado	\$ 930,00

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

En vista de que algunas medidas para la seguridad de la información se lo realiza una sola vez, en las entidades del segmento cuatro para los años siguientes el presupuesto anual estimado es de \$ 930,00



Con el fin de proporcionar una guía y apoyo a la dirección en temas de seguridad de la información, a continuación a modo orientativo se presenta la solución frente a los problemas más comunes detectados en las entidades Incluye aquellas dedicadas a las actividades Administrativas y de Apoyo, Enseñanza, Salud y de Alojamiento

PROBLEMAS DE SEGURIDAD DE LA INFORMACIÓN

142

1. Ausencia de políticas de puesto de trabajo despejado y bloqueo de pantalla automático.
 2. Ausencia de políticas de seguridad de la información para proveedores.
 3. Se comunica las fallas de S.I. a todo el personal
 4. No se da de baja a los accesos de los empleados una vez que termine el contrato laboral.
 5. Los acuerdos de confidencialidad se firman después de iniciar las labores o incluso no se firman este tipo de acuerdos.
 6. Los sistemas a ser implementados no son revisados inicialmente.
 7. Ataque o infección por código malicioso.
 8. Robo/acceso a la información.
 9. Interrupción prolongada en un sistema o servicio de red.
 10. Intento de acceso a un sistema informático.
 11. Robo de equipos
 12. Uso indebido de información crítica
 13. No tienen un método o programa para borrar la información confidencial
 14. No se dispone de un registro de los intentos de accesos fallidos y exitosos del sistema.
 15. Administración y control de red / ingreso al sistema de otras áreas
 16. Software sin licencias originales.
 17. No se realizan copias de seguridad de toda la información sensible de la empresa.
 18. No cuentan con un gestor de contraseñas
 19. Actualización automática del sistema operativo.
 20. No tienen restricciones en el uso de internet.
 21. Áreas seguras sin control de ingreso.
- (Información tomada de las encuestas)

POLÍTICAS DE SEGURIDAD PARA PROTEGER LA INFORMACIÓN

Políticas	Lineamientos
1. Asegurar la integridad y la confidencialidad de la información que maneja la entidad.	1. 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.
2. La información que maneja el personal debe ser protegida en cualquiera de sus formas una vez que el usuario abandone su puesto de trabajo.	2. Cada vez que el usuario se ausente de su puesto de trabajo, se debe activar el protector de pantalla definido y a su vez debe guardar en un lugar seguro cualquier documento y medios que contengan información confidencial y de uso interno.
3. Todo proveedor de la entidad podrá desarrollar para la empresa aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios, acatando con responsabilidad cada uno de los acuerdos, lineamientos y normativas que imponga la empresa.	3. Realizar la formalización de un acuerdo escrito de confidencialidad debidamente firmado entre las partes antes de efectuar las actividades técnicas contratadas a empresas externas de modo que la información no podrá ser utilizada en ningún caso fuera del marco establecido.

Políticas

4. Todo comunicado que se efectuó en la entidad debe ser transmitido únicamente al personal correspondiente
5. Una vez confirmado que han cesado las funciones del empleado se debe dar de baja al usuario en el acceso a los sistemas de información.
6. Preparar un respaldo legal para proteger la información que se utiliza por los empleados durante las actividades laborales.
7. Para garantizar la calidad del equipo o software adquirido, el personal encargado del área de Seguridad de la Información revisará inicialmente el producto antes de su implementación, en caso de no contar con un experto propio de la empresa, se podrá recurrir a los servicios externos.
8. Realizar un registro documental ordenado y valorada de los elementos que comprenden los activos de la información
9. Eliminación o destrucción segura de la información confidencial de la empresa.
10. Mantener procesos de auditoría basada en la revisión de logs que muestran las actividades realizadas por el usuario sobre un sistema con el objetivo de asegurar el funcionamiento operacional de la seguridad en un sistema.

Lineamientos

4. 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.
5. Para ello se le debe retirar inmediatamente el computador, el teléfono, la tarjeta de acceso, y deshabilitar el usuario y contraseña de la cuenta del sistema de información que utilizaba en el tiempo de labores.
6. Presentar acuerdos escritos de confidencialidad en donde el empleado se comprometa a no revelar a personas ajenas a la empresa la información que maneja.
7. Verificar que tanto el equipo, así como también el software cumplan con los estándares adecuados y que ejecuten las funciones previstas. Además necesariamente se deberá comprobar de que el software mantenga las medidas de seguridad que permitan detectar códigos maliciosos, virus informáticos y demás que pueden provocar la pérdida de la información.
8. Para realizar un inventario de activos de información se puede iniciar clasificando en activos de información pura, activos físicos y activos humanos.
9. 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.
10. Mantener un registro de intento de accesos fallidos al iniciar sesión, así también registrar los usuarios que no ingresaron la contraseña correcta después algunos intentos, bloquear el ID de usuario en caso de que sobrepase tres intentos de acceso.



Políticas

11. 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.
12. El usuario del sistema podrá acceder a los permisos que un desarrollador otorga sobre el sistema.
13. Para asegurar la integridad y la disponibilidad de la información se requiere periódicamente aplicar sistemas de Backup.
14. Las nuevas implementaciones o actualizaciones de software debe estar sujetas a revisión.
15. Controlar a los usuarios el acceso a los servicios de internet

Lineamientos

11. 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.
12. Firmar un contrato entre el titular con derechos de la propiedad intelectual y el usuario, por lo que previamente los programas serán valorados.
13. Cuando se va a realizar copias de seguridad de la información se debe identificar el tipo de copias y la periodicidad de las mismas, así como los soportes en las que se deben realizar y las ubicaciones de los centros de respaldo.
14. Toda actualización del sistema operativo debe ser revisada su compatibilidad con los programas que utiliza la empresa para su posterior instalación en los equipos.
15. Determinar las direcciones a las cuales el usuario puede ingresar



SOLUCIÓN	COSTOS
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por cada máquina	\$ 40,00
Responsabilidades de gestión	
8 Cámaras de seguridad	\$ 800,00
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 (DOMINIO)	\$ 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	\$ 20,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Controles de acceso	
Equipo servidor	\$ 2.000,00
Configuraciones (ACL)	\$ 800,00



PRESUPUESTO ESTIMADO IMPLEMENTACIÓN –De problemas más comunes de las empresas del sector.

SOLUCIÓN	COSTOS
Políticas de uso de controles criptográficos	
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 máquinas	\$ 400,00
Gestión de contraseñas de usuario	
Gestor de contraseñas	\$ 20,00
Protección de los registros de información	
Equipo servidor	\$ 2000,00
Configuraciones	\$ 1500,00
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
Total Presupuesto de Inversión	\$ 6660,00

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

En base a los incidentes y los controles de seguridad de la información no aplicados mayormente en las entidades reguladas por la Superintendencia de Compañías, el presupuesto estimado para la empresa que por primera vez busca implementar medidas para la seguridad de la información, el monto aproximado de presupuesto para el año 1 es de 6.660,00 dólares

PRESUPUESTO ANUAL ESTIMADO (Para años siguientes)

146

SOLUCIÓN	COSTOS
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 cada máquina	\$ 400,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina	\$ 70,00
Licencia Paquete Office por máquina	\$ 90,00
Total Presupuesto de Inversión	\$ 960,00

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

En vista de que algunas medidas para la seguridad de la información se lo realizan una sola vez, en las entidades reguladas por la Superintendencia de Compañías para los años siguientes el presupuesto anual estimado es de \$ 960,00



RETORNO DE LA INVERSIÓN EN SEGURIDAD DE LA INFORMACIÓN

(ROSI)

Indicador que nos permite determinar si una inversión en seguridad es rentable desde el punto de vista financiero de modo que los costos en seguridad sean menor que el activo que se protege.

A continuación se presenta el cálculo del Beneficio Marginal que se obtiene a través del indicador ROSI, para lo cual se ha considerado los problemas de seguridad mayormente ocurridos en las empresas.

Para el cálculo del beneficio se utilizó el costo que represento enmendar los problemas de seguridad, así mismo se trabajó con el presupuesto estimado de implementación y considerando un riesgo de mitigación en base al número de incidentes,

La información fue obtenida de las encuestas realizadas.

FÓRMULA:

$$\text{ROSI} = \frac{[(\text{Riesgo de exposición} * \% \text{ Riesgo mitigado}) - \text{Costos de inversión}]}{\text{Costos de inversión}}$$

SOLUCIÓN	COSTO
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Configuración Red inalámbrica y red local	\$ 200,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Concienciación, educación y capacitación en S.I	
Charla sobre Ingeniería social, fraude o phishing, un día.	\$ 200,00
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Firewall Empresarial + compra de equipo	\$ 3.000,00
Licencia Anual Firewall	\$ 5.000,00
Total Presupuesto de Inversión	\$ 9.030,00

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

CÁLCULO DEL ROSI

DATOS:

- Número de problemas= 6
- Coste del incidente=\$20.000 (Riesgo de exposición) / (Dato de la encuesta)
- Costo solución =\$ 9.030
- % Riesgo Mitigado =83,33%

ROSI= [(Riesgo de exposición * % Riesgo mitigado) – Costos de inversión] / Costos de inversión

$$\text{ROSI} = [(\$20.000 * 83,33\%) - \$9.030] / \$9.030$$

$$\text{ROSI} = 84,56\% (\$0,84)$$

INTERPRETACIÓN

Asumiendo que el costo anual promedio de los problemas mayormente ocurridos en la cooperativa del segmento uno es de \$20.000 dólares, y que las medidas adoptadas de solución contendrán el 83,33% de los incidentes, se demuestra que la inversión de \$9.030 para la seguridad de la información tiene un retorno esperado de 84,56%, es decir que por cada dólar que se invierte en S.I, se puede dejar de perder \$ 0,84 dólares.

SOLUCIÓN	COSTO
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	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal 25 maquina	\$ 1.000,00
Derechos de propiedad intelectual	
Licencia del sistema operativo por máquina 25 máquinas	\$ 1.750,00
Licencia Paquete Office por máquina 25 máquinas	\$ 2.250,00
Total Presupuesto de Inversión	\$ 5.730,00

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

CÁLCULO DEL ROSI

DATOS:

- Número de problemas más comunes = 5
- Coste del incidente=\$15.000 (Riesgo de exposición) / (Dato de la encuesta)
- Costo solución =\$ 5.730
- % Riesgo Mitigado = 80,00%

ROSI= [(Riesgo de exposición * % Riesgo mitigado) – Costos de inversión] / Costos de inversión

$$\text{ROSI} = [(\$15.000 * 80,00\%) - \$5.730] / \$5.730$$

$$\text{ROSI} = 109,42\% (\$1,09)$$

INTERPRETACIÓN

Asumiendo que el costo anual promedio de los incidentes mayormente ocurridos en la cooperativa del segmento dos es de \$15.000 dólares, y que las medidas adoptadas de solución contendrán el 80,00% de los incidentes, se demuestra que la inversión de \$5.730 para la seguridad de la información tiene un retorno esperado de 109,42%, es decir que por cada dólar que se invierte en S.I, se puede dejar de perder \$ 1,09 dólares.



SEGMENTO 2

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

SOLUCIÓN	COSTOS
Políticas de uso de controles criptográficos	
Criptografía para página Web	\$ 130,00
Configuración Red inalámbrica y red local	\$ 200,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal 15 por máquina	\$ 600,00
Responsabilidades de gestión	
8 Cámaras de seguridad	\$ 800,00
Gestión de contraseñas de usuario	
Gestor de contraseñas	\$ 20,00
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Charla sobre el uso indebido de la información crítica	\$ 200,00
Procedimientos seguros de inicio de sesión	
Roles, logs, Integridad por cifrado	\$ 3.000,00
Total Presupuesto de Inversión	\$ 5.350,00

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

CÁLCULO DEL ROSI

DATOS:

- Número de problemas más comunes=11
- Coste del incidente=\$12.000 (Riesgo de exposición) / (Dato de la encuesta)
- Costo solución =\$ 5.350
- % Riesgo Mitigado = 90,91%

ROSI = [(Riesgo de exposición * % Riesgo mitigado) – Costos de inversión] / Costos de inversión

$$\text{ROSI} = [(\$12.000 * 90,91\%) - \$5.350] / \$5.350$$

$$\text{ROSI} = 103,91\% (\$1,03)$$

INTERPRETACIÓN

Asumiendo que el costo anual promedio de los incidentes mayormente ocurridos en la cooperativa del segmento tres es de \$12.000 dólares, y que las medidas adoptadas de solución contendrán el 90,91% de los incidentes, se demuestra que la inversión de \$5.350 para la seguridad de la información tiene un retorno esperado de 103,91%, es decir que por cada dólar que se invierte en S.I, se puede dejar de perder \$ 1,03 dólares.



SEGMENTO 3

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

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	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 máquina	\$ 400,00
Eliminación de Soportes	
Método o programa para el borrado de información confidencial	\$ 24,00
Segregación de redes	
Router	\$ 500,00
Switch	\$ 200,00
Rack	\$ 400,00
Patch Panel	\$ 80,00
Configuraciones	\$1.000,00
Gestión de contraseñas de usuario	
Gestor de contraseñas manual	\$ 20,00
Gestión de capacidades/Actualización del sistema operativo	
Configuraciones	\$ 100,00
Controles físicos de entrada	
Lector biométrico	\$ 400,00
Total Presupuesto estimado implementación	\$ 3.854,00

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

CÁLCULO DEL ROSI

DATOS:

- Número de problemas más comunes= 14
- Coste del incidente=\$9.000 (Riesgo de exposición) / (Datos de la encuesta)
- Costo solución =\$ 3.854
- % Riesgo Mitigado = 92,86%

ROSI= [(Riesgo de exposición * % Riesgo mitigado) – Costos de inversión] / Costos de inversión

$$\text{ROSI} = [(\$9.000 * 92,86\%) - \$3.854] / \$3.854$$

$$\text{ROSI} = 116,85\% (\$1,16)$$

INTERPRETACIÓN

Asumiendo que el costo anual promedio de los incidentes mayormente ocurridos en las cooperativas del segmento cuatro es de \$9.000 dólares, y que las medidas adoptadas de solución contendrán el 92,86% de los incidentes, se demuestra que la inversión de \$3.854 para la seguridad de la información tiene un retorno esperado de 116,85%, es decir que por cada dólar que se invierte en S.I, se puede dejar de perder \$ 1,16 dólares.

SOLUCIÓN	COSTOS
Concienciación, educación y capacitación en S.I	
Capacitación en procedimientos de seguridad de la información.	\$ 400,00
Controles contra el código malicioso	
Antivirus + licencia + firewall personal por 10 máquinas	\$ 400,00
Gestión de contraseñas de usuario	
Gestor de contraseñas	\$ 20,00
Protección de los registros de información	
Equipo servidor	\$ 2000,00
Configuraciones	\$ 1500,00
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
Total Presupuesto de Inversión	\$ 6.660,00

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

CÁLCULO DEL ROSI

DATOS:

- Número de incidentes más comunes=11
- Coste del incidente=\$15.000 (Riesgo de exposición) / (Dato de la encuesta)
- Costo solución =\$ 6.660
- % Riesgo Mitigado = 90,91%

ROSI= [(Riesgo de exposición * % Riesgo mitigado) – Costos de inversión] / Costos de inversión

$$\text{ROSI} = [(\$15.000 * 90,91\%) - \$6.660] / \$6.660$$

$$\text{ROSI} = 104,75\% (\$1,04)$$

INTERPRETACIÓN

Asumiendo que el costo anual promedio de los incidentes mayormente ocurridos en las empresas reguladas por la Superintendencia de Compañías es de \$15.000 dólares, y que las medidas adoptadas de solución contendrán el 90,91% de los incidentes, se demuestra que la inversión de \$6.990 para la seguridad de la información tiene un retorno esperado de 104,75%, es decir que por cada dólar que se invierte en S.I, se puede dejar de perder \$ 1,04 dólares.



En cumplimiento al cuarto objetivo “Establecer el costo y el beneficio marginal de invertir en herramientas de seguridad y protección de datos que utilizan las empresas del sector servicios”. Se elaboró una matriz detallada de los costos y el beneficio marginal, permitiendo evaluar el impacto económico de la inversión.

5.5.2. FASE II Elaborar una matriz costo-beneficio

Tabla 49

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%

FASE III Desarrollar un simulador de inversión

En cumplimiento del último objetivo de la presente investigación, se diseña un simulador de inversión, que ayude principalmente a la administración de las empresas del sector servicios en la toma de decisiones, con respecto a la adquisición de herramientas o mecanismos de seguridad y protección de datos.

La construcción del modelo inicia con una portada en el que se destaca cuatro puntos muy importantes:



Figura 40. Simulador- Hoja de contenidos

a) Generalidades

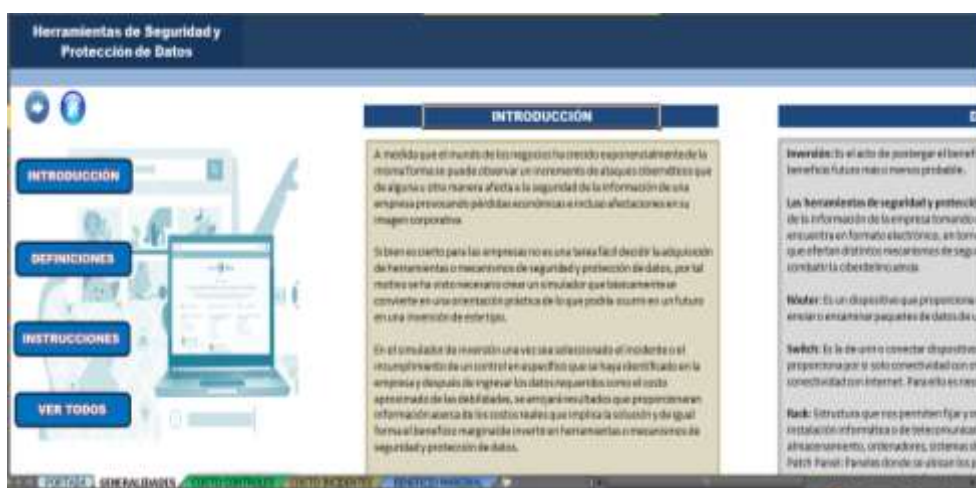


Figura 41 .Simulador – Hoja de Generalidades

En esta plantilla usted podrá visualizar una breve introducción, además de algunas definiciones básicas que permitirán aclarar dudas, así también se tiene la opción de contar con instrucciones necesarias para el manejo del simulador.

Introducción


A medida que el mundo de los negocios ha crecido exponencialmente de la misma forma se puede observar un incremento de ataques cibernéticos que de alguna u otra manera afecta a la seguridad de la información de una empresa provocando pérdidas económicas e incluso afectaciones en su imagen corporativa

Si bien es cierto para las empresas no es una tarea fácil decidir la adquisición de herramientas o mecanismos de seguridad y protección de datos, por tal motivo se ha visto necesario crear un simulador que básicamente se convierte en una orientación práctica de lo que podría ocurrir en un futuro en una inversión de este tipo.

En el simulador de inversión una vez sea seleccionado el incidente o el incumplimiento de un control en específico que se haya identificado en la empresa y después de ingresar los datos requeridos como el costo aproximado de las debilidades, se arrojará resultados que proporcionaran información acerca de los costos reales que implica la solución y de igual forma el beneficio marginal de invertir en herramientas o mecanismos de seguridad y protección de datos.

Los resultados generados permitirán especialmente a la administración de la empresa tomar decisiones acertadas al momento de invertir en este tipo de productos en función de las necesidades y capacidades de la empresa.

Definiciones

 **Róuter:** Es una herramienta que proporciona conectividad a nivel de red, Su finalidad consiste en enviar paquetes de datos de una red a otra.

- ✚ **Switch:** conecta y une dispositivos en red. Se debe considerar que un switch no proporciona por si solo conectividad con otras redes, y tampoco proporciona conectividad con Internet. Para ello es indispensable un router.
- ✚ **Rack:** Estructura que nos permiten fijar y organizar, equipos como servidores, ordenadores, sistemas de redes, switches, sistemas de almacenamiento, etc.
- ✚ **Patch Panel:** Paneles donde se encuentran los puertos de una red, que estan localizados en un rack.
- ✚ **Sistema Backup:** Mecanismo para el almacenamiento de copias de seguridad de la información.
- ✚ **Criptografía:** Método que protege documentos y datos. A través del uso de cifras o códigos.

Instrucciones

1. Seleccione el organismo de control a la cual se sujeta la entidad, así también se debe elegir el tipo de segmento financiero o actividades a la que se dedica la empresa.
2. Selecciona las debilidades y el tipo de incidentes o brechas de seguridad que se ha detectado en tu empresa e inmediatamente te arrojará herramientas o mecanismos de seguridad y protección de datos, enseguida mostrará los costos unitarios
3. En ocasiones deberás especificar el número de ordenadores que dispone actualmente tu empresa y obtendrás el costo total de la solución.
4. Una vez completados estos pasos en la Hoja Beneficio marginal debes ingresar los costos de los problemas de S.I.
5. Una vez ingresado los incidentes, costos de reparación y los costos de solución el simulador te arrojará el beneficio marginal utilizando el indicador ROSI (Retorno sobre la Inversión de Seguridad.).
6. Adicionalmente en el simulador detectará como alertas en caso de que el beneficio sea negativo dando a conocer que la inversión no es factible,

caso contrario si el beneficio es positivo se recomienda a la administración adquirir la herramienta o mecanismo de seguridad.

b) Costo / controles

HERRAMIENTAS Y MEDIDAS DE SEGURIDAD Y PROTECCIÓN DE DATOS PARA MITIGAR CONTROLES ISO 27002				
Elegir los controles en control de la seguridad de la información				
Control Norma ISO 27002	Herramientas	Cantidad	Costo Unit.	Costo Total
Ausencia de política de uso de controles	Capacidad de procedimientos de seguridad de la información	1	40,00	40,00
...
...
...
...

Figura 42. Hoja controles ISO 27002 - Herramientas

En esta plantilla se debe seleccionar el tipo de empresa o segmento financiero al cual pertenece la empresa, así también se tiene la opción de seleccionar los controles de la Norma ISO 27002 que no se aplica actualmente en la entidad y se procede a realizar la programación de la simulación dando a conocer el costo total de aplicar los controles de seguridad.

c) Costo / incidentes

COSTOS DE LAS HERRAMIENTAS Y MEDIDAS DE SEGURIDAD Y PROTECCIÓN DE DATOS		
Elegir los incidentes de seguridad que se han producido en la empresa		
Incidentes de Seguridad	Herramientas	Costo
Ataque o infección por Código Malicioso	Actividad + Servicio + Personal personal por cada ataque	40,00
...
...
...
...

Figura 43. Simulador Hoja de incidentes

En esta plantilla inicialmente se debe seleccionar el organismo de control al que está sujeta la empresa de servicios bien podría ser la Superintendencia de Compañías o la Superintendencia de Economía Popular y Solidaria, así también se debe seleccionar el tipo de actividad o el segmento cooperativo al cual pertenece.

Seguidamente debe seleccionar los incidentes o brechas de seguridad que se ha detectado en la empresa, los incidentes definidos en el simulador son:

- Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)
- Modificación o eliminación no autorizada de datos.
- Robo de la información.
- Interrupción prolongada en un sistema o servicio de red.
- Acceso o intento de acceso no autorizado a un sistema informático.
- Ingeniería social, fraude o phishing.
- Destrucción no autorizada de información.
- Robo de equipos.
- Uso indebido de información crítica

Herramientas de Seguridad y Protección de Datos 

MATRIZ DE COSTOS / PRESUPUESTO INVERSIÓN

 Ingrese cantidad en función de su requerimiento

Incidentes de seguridad	Herramientas	Cantidad	Costo
Ataque o infección por código malicioso	Antivirus + licencia + Firewall personal por cada máquina	25	40,00 1.000,00
FAUSO	Charla sobre Ingeniería social, fraude o phishing, en día	1	-
Robo de equipos	3 Cámaras de seguridad	3	80,00 240,00
FAUSO	Charla sobre uso indebido de la información crítica	1	-
FAUSO			

PLANTILLA INCIDENTES

Figura 44. Hoja incidentes – Matriz Costo

Una vez definidas los incidentes de seguridad, se procede a realizar la programación de la simulación e inmediatamente da como resultado las herramientas o mecanismos que la empresa debe implementar para contrarrestar los efectos producidos y evitar que de nuevo la empresa se vea afectada por el mismo incidente una y otra vez. Así también arrojará los costos unitarios que representa la solución, y en el caso que lo amerite debe ingresar la cantidad de ordenadores que dispone en su empresa y conseguirá el costo total por incidente, al finalizar obtendrá completa la matriz con los costos totales de las herramientas por todos los incidentes encontrados.

d) Beneficio marginal

Figura 45. Hoja Beneficio –Matriz Beneficio

Seguidamente se debe ingresar los costos que representa reparar el daño y una vez establecido el número de incidentes, los costos de la solución obtenidos con el simulador, y el porcentaje del riesgo mitigado que si bien es cierto un riesgo no se puede eliminar por completo pero debe ser minimizado, con todos estos datos se obtendrá inmediatamente el beneficio marginal utilizando el indicador ROSI (Retorno sobre la Inversión en Seguridad).

	Porcentaje negativo = Rechazo la inversión
	Porcentaje positivo = Acepto la inversión

El simulador dará a conocer una alerta, si el beneficio porcentual es negativo se tornara un color rojo y un mensaje que rechaza la inversión, caso contrario si el beneficio porcentual es positivo se tornara un color verde y un mensaje que puede aceptar la inversión.

El simulador construido es de fácil manejo, y sobre todo práctico porque sirve como experimentación de lo que puede suceder a futuro con diferentes comportamientos, los resultados arrojados por el software, analizan el costo/beneficio de invertir en herramientas de seguridad y protección de datos, dichos resultados varían dependiendo de los incidentes ocurridos en la empresa, en definitiva el simulador orienta a la mejora en optimización de recursos y rentabilidad.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

Una vez realizado el estudio de campo a las empresas reguladas por la Superintendencia de Economía Popular y Solidaria del segmento uno, dos, tres y cuatro, adicionalmente a las empresas dedicadas a las actividades: administrativas y de apoyo, enseñanza, salud y alojamiento reguladas por la Superintendencia de Compañías, se determinó que la inversión en herramientas de seguridad y protección de datos genera un costo-beneficio marginal a las empresas de estos sectores.

6.1 Conclusiones

En cumplimiento con los objetivos propuestos de la presente investigación se obtuvo las siguientes conclusiones:

- Al iniciar el estudio de inversión en Herramientas de Seguridad y protección de Datos, al analizar el 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.
- Se establece que la inversión en la cuenta de equipo de cómputo y software dentro del período 2012-2016 tuvo un nivel de crecimiento considerable, en promedio en el segmento uno se observó un 14,89%; en el segmento dos 15,54%; en el segmento tres 18,26%, en el segmento cuatro 7,57% y finalmente en las empresas reguladas por la SC reflejan un crecimiento de 16,04%, esta información es relevante para la investigación porque de ahí surge la necesidad de aplicar herramientas y medidas de seguridad que protejan la información.
- Actualmente son 13 empresas de servicios que en función de su organigrama la Gerencia General es responsable de velar por la seguridad de la información, de este grupo 9 empresas corresponden al segmento cuatro de las cooperativas de ahorro y crédito, debido al

desconocimiento en protección de activos de la información por parte de la Gerencia, tienen la necesidad de contratar servicios de externalización.

- 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 de código malicioso por año, siendo evidente que la herramienta utilizada, no ayuda a combatir el incidente.
- 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 permitiendo un fácil acceso a la información de otros departamentos, el 61,54% no utilizan un gestor de contraseñas que aseguren su almacenamiento y garanticen usuarios y contraseñas únicas, el 61,54% los ordenadores se actualizan automáticamente impidiendo verificar la compatibilidad con el Sistema operativo y demás aplicaciones del sistema, y el 80,77% comunica los eventos de inseguridad a todo el personal provocando conmoción.
- Tras la obtención de resultados se determinó que las entidades del segmento uno para hacer frente a los incidentes requieren un costo promedio de inversión de \$9.300 obteniendo un beneficio marginal de 84.56%, así también las cooperativas del segmento dos necesitan un costo promedio de inversión de \$5.730 obteniendo un beneficio marginal de 109.42%, en el segmento tres el costo promedio de inversión es de \$5.350 con un beneficio marginal de 103.91%, en el segmento cuatro se requiere un costo promedio de inversión de \$3.854 obteniendo un beneficio marginal de 116.85%, por último las empresas reguladas por la SC deben asignar un costo promedio de inversión de \$6.660, alcanzando un beneficio de 104,75%, esto quiere decir que en todos los casos de estudio la inversión es fiable con un retorno positivo, cabe considerar que

el beneficio porcentual calculado representa lo que una empresa dejaría de perder por cada dólar que invierte en seguridad de la información.

- 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 lo tanto se puede evidenciar que en ambos segmentos se maneja una buena gestión para proteger los activos de la información, sin embargo al tener pocos problemas, los resultados de la encuesta indican un costo alto por los incidentes, 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, estos resultados indican que para la administración de estas empresas no se da prioridad a la gestión e inversiones en tecnología, considerando además que el costo de los incidentes de estas empresas son menores pese a que tuvieron un número elevado de incidentes.

6.2. Recomendaciones

Con relación a las conclusiones anteriormente desarrolladas se establecen las siguientes 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.
- Al presenciar un crecimiento en equipo de cómputo necesariamente se debe gestionar herramientas o mecanismos de seguridad que hagan frente a las vulnerabilidades encontradas, caso contrario el equipo informático al no contar con la protección adecuada aumenta las probabilidades de daño, modificación, o pérdida de la información.

- Se recomienda a las empresas del sector servicios una vez que su participación sea estable en el mercado, gestionar la creación de un área/departamento encargado de los sistemas y tecnologías de la información, evitando el incumplimiento de los acuerdos de confidencialidad al contratar servicios de externalización.
- 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.
- 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.
- Se recomienda a las empresas del segmento tres, cuatro y las entidades dedicadas a actividades de alojamiento, administrativas, educación y salud, contar con asistencia técnica especializada para evaluar la adquisición de herramientas de seguridad acopladas a los requerimientos y problemas detectadas en las entidades, servicios externalización como son pequeñas no es necesario un departamento propio de tecnología para evitar gastos innecesarios
- 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.

SIGLAS Y ABREVIATURAS

ISO: Organización Internacional de Normalización

SEPS: Superintendencia de Economía Popular y Solidaria

SC: Superintendencia de Compañías

COAC: Cooperativa de ahorro y Crédito

ROSI: Retorno de la Inversión en Seguridad

SFPS: Sistema financiero Popular y Solidario

ACL: Access Control List (Lista de control de Acceso)

SI: Seguridad de la Información

REFERENCIAS BIBLIOGRÁFICAS

- Hernández Sampieri, R., Baptista Lucio, M., & Férnandez Collado, C. (2010). *Metodología de la Investigación* (Vol. Quinta Edición). (S. D. McGraw-Hill / Interamericana Editores, Ed.) México, D.F.: ISBN 978-607-15-0291-9.
- Multicomp. (2011). *Multicomp*. Recuperado el 13 de febrero de 2018, obtenido de: <http://multicomp.com.mx/seguridad-it-invertir-o-convencer-para-invertir-he-ahi-el-dilema-1-de-3/>
- Computing. (2016). *COMPUTING*. Recuperado el 26 de enero de 2018, obtenido de: <http://www.computing.es/seguridad/informes/1094283002501/segun-un-informe-de-gartner-muchas-empresas-equiparan-erroneamente-el-gasto-de-seguridad-ti-con-la-madurez.1.html>
- Portafolio*. (05 de 2017). Recuperado el 15 de febrero de 2018, de <http://www.portafolio.co/tendencias/la-ciberseguridad-un-tema-de-cultura-y-sensibilizacion-en-las-empresas-506011>
- Superintendencia de Compañías*. (2018). Recuperado el 25 de marzo de 2018, de <https://portal.supercias.gob.ec/wps/portal/Inicio/Institucion>
- Superintendencia de la Economía Popular y Solidaria*. (2018). Recuperado el 28 de marzo de 2018, de <http://www.seps.gob.ec/interna?-que-es-la-seps->
- Aguilera, P. (2010). *Seguridad Informática*. Editex: ISBN. 8497717619, 9788497717618
- Albarracín, C. (12 de 2011). *Google Academico* . Recuperado el 16 dde diciembre del 2018. Obtenido de <http://repositorio.uisrael.edu.ec/bitstream/47000/167/1/UISRAEL-EC-SIS-378.242-403.pdf>
- Andersson, B. (05 de 2017). *Expreso.ec*. Recuperado el 27 de diciembre del 2018. Obtenido de <http://www.expreso.ec/actualidad/ecuador-y-casi-100-paises-sufren-ciberataque-extorsivo-HJ1319548>
- Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. España : Cengage Learning Paraninfo. ISBN: 8497325028, 9788497325028
- Arias, F. (2012). *El proyecto de investigación*. (l. 980-07-8529-9, Ed.) Caracas: EPISTEME, C.A.

- Asensio, G. (2006). *Seguridad en Internet (: Una guía práctica y eficaz para proteger su PC con software gratuito)*. Madrid: Nowtilus, S.L.
- Ávila, R. (2016). *DINERO*. Recuperado el 18 de septiembre de 2017, Obtenido de:
<https://www.dinero.com/Buscador?query=encuesta%20anual%20de%20seguridad%20de%20la>
- BBVA. (2017). *¿Qué es la inversión? | BBVA*. Recuperado el 26 de enero de 2018, Obtenido de: <https://www.bbva.com/es/que-es-la-inversion/>
- Bermúdez, K. G., & Bailón, E. R. (2015). *Repositorio Digital-UPS*. Recuperado el 06 de febrero del 2018. Obtenido de
<https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf>
- Bortnick, S. (2010). *Welivesecurity*. Recuperado el 21 de septiembre de 2017, Obtenido de: <https://www.welivesecurity.com/la-es/2010/04/06/retorno-de-inversion-en-seguridad/>
- Cárdenas, J. (2015). *Repositorio Institucional UNIANDES*. Recuperado el 12 de diciembre del 2017. Obtenido de
<http://dspace.uniandes.edu.ec/bitstream/123456789/579/1/TUAMEIEO07-2015.pdf>
- Chacón Krisia. (06 de 2016). *El Financiero*. Recuperado el 12 de septiembre de 2017. Obtenido de:
http://www.elfinancierocr.com/tecnologia/ciber crimen-negocio-toma-potencia-region_0_976102388.html
- Clase & Calidad. (2013). *Consultoría en Crecimiento de PYMES y Empresas Familiares*. Recuperado el 24 de enero de 2018, Obtenido de:
<http://www.clasec.net/como-hacer-presupuestos-parte-3-presupuesto-de-inversiones/>
- Código Orgánico Integral Penal. (2014). *Ministerio de Justicia Derechos Humanos y Cultos*. Recuperado el 17 de marzo del 2018. Obtenido de
http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf
- Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador*. Recuperado el 19 de Diciembre del 2017. Obtenido de
http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolillo.pdf

- Corral, Y. (2009). Validez y confiabilidad de los instrumentos de investigación para la recolección de datos. *Revista ciencias de la educación*, 25.
- Diario El Mundo. (06 de 2015). *El Mundo*. Recuperado el 27 de agosto de 2017, Obtenido de: <http://elmundo.sv/el-60-de-las-empresas-que-pierden-datos-cierra/>
- Editor. (12 de 2017). *WeLiveSecurity*. Recuperado el 12 de septiembre de 2017. Obtenido de: <https://www.welivesecurity.com/la-es/2017/12/20/gasto-seguridad-empresas-continua-aumento/>
- Flores, F. G. (2007). Repositorio Universidad Técnica de Ambato. *Estudio, Administración e Implementación de Políticas de Seguridad en la Red*. Recuperado el 15 de enero del 2018. Obtenido de <http://repositorio.uta.edu.ec/bitstream/123456789/211/1/t289si.pdf>
- Gómez, Á. (2011). *Enciclopedia de la Seguridad Informática*. España: Grupo Editorial RA-MA.
- Gonzalez, W. (2009). *Recolección de Datos*. Recuperado el 19 de febrero del 2018. Obtenido de <http://recodatos.blogspot.com/2009/05/tecnicas-de-recoleccion-de-datos.html>
- Guzmán, A. (2011). *Seguridad informática*. Recuperado el 23 de enero de 2018. Obtenido de <http://seguridadanggie.blogspot.com/2011/11/incidente-de-seguridad.html>
- ISOTools. (2015). *La familia de normas ISO 27000*. Recuperado el 16 de octubre de 2017. Obtenido de <https://www.isotools.org/2015/01/21/familia-normas-iso-27000/>
- Kroustek Jakub. (05 de 2017). *20 Minutos*. Recuperado el 23 de agosto de 2017. Obtenido de <http://www.20minutos.es/noticia/3036319/0/vulnerabilidad-windows-pone-jaque-seguridad-informatica-mundial/>
- Paredes J. (13 de febrero de 2015). *La Razón*. Cada mes se hackean los sistemas informáticos de unas 15 empresas. Recuperado el 12 de marzo del 2018. Obtenido de http://www.la-razon.com/economia/mes-hackean-sistemas-informaticos-empresas_0_2216778323.html
- Ley del Sistema Nacional de Registro de datos Públicos. (2012). *Ley del Sistema Nacional de Registro de datos Públicos*. Obtenido de <https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf>

- Ley Orgánica de la gestión de la Identidad y Datos Civiles. (2016). *Ley Orgánica de la gestión de la Identidad y Datos Civiles*. Obtenido de https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2016/03/LEY_ORGANICA_RC_2016.pdf
- Ley Orgánica de Transparencia y Acceso a la Información Pública. (2004). *Ley Orgánica de Transparencia y Acceso a la Información Pública*. Obtenido de http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf
- López, A., & Ruiz, J. (2012). *El portal de ISO 27002 en Español*. Recuperado el 25 de octubre de 2017. Obtenido de <http://www.iso27000.es/iso27002.html>
- Madarri, A., Archenti, N., & Piovani, J. (2007). *Metodología de la Ciencias Sociales* (328 ed.). Buenos Aires: Emecé.
- Moreno Anaya, E. (2013). *Instrumentos de Investigación*. Recuperado el 29 de marzo del 2018. Obtenido de <https://prezi.com/ntpf0m3pxyuh/instrumentos-de-investigacion/>
- Ortega, J. (01 de 2015). *El Comercio*. Recuperado el 21 de septiembre de 2017. Obtenido de <http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html>
- Proyecto de Ley Organica de la Proteccion de los Derechos a la Intimidad y Privacidad sobre los Datos Personales. (2016). Obtenido de: <file:///C:/Users/PERSONAL/Desktop/Proyecto-de-Ley-Organica-de-la-Proteccion-de-los-Derechos-a-la-Intimidad-y-Privacidad-sobre-los-Datos-Personales.pdf>
- Rodríguez, M. L. (2013). *Plataforma de Metodología de la Investigación Científica y para la Guía de Tesis de Grado*. Recuperado el 04 de 09 de 2017. Obtenido de: <https://guiadetesis.wordpress.com/2013/08/19/acerca-de-la-investigacion-bibliografica-y-documental/#comments>
- Ruiz, M., & Vargas, J. (2008). *Fuentes de Información*. Obtenido de <http://ponce.inter.edu/cai/manuales/FUENTES-PRIMARIA.pdf>
- Sánchez, L. A. (2015). *Repositorio Institucional UNIANDES*. Modelo de Gestión para el Desarrollo de Procesos de Seguridad en la Red de Datos de la Cooperativa de Ahorro y Crédito Guaranda Ltda. Recuperado el 10 de enero del 2018. Obtenido de: <http://dspace.uniandes.edu.ec/bitstream/123456789/581/1/TUAMEIE09-2015.pdf>

Secretaría Nacional de Planificación y Desarrollo. (2013). *Secretaría Nacional de Planificación y Desarrollo*. Recuperado el 15 de agosto del 2017. Obtenido de <http://www.buenvivir.gob.ec/objetivos-nacionales-para-el-buen-vivir>

Sosa Johana. (2012). *Google Scholar* .Clasificación de la información. Recuperado el 12 de febrero del 2018, Obtenido de: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Clasificacion_de_la_Informacion.pdf

ANEXOS



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

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORIA

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por la señorita **TANIA STEFANÍA COFRE SANTO** y por la señorita **VICTORIA CAROLINA REMACHE SOTO**.

En la ciudad de Latacunga, a los 7 días del mes de mayo 2018.

Aprobado por:


Econ. Francisco Caicedo A.

DIRECTOR DEL PROYECTO



Econ. Alisva Cárdenas

DIRECTORA DE CARRERA (e).





Dr. Freddy Jaramillo

SECRETARIO ACADÉMICO