



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN INNOVACIÓN Y
TRANSFERENCIA DE TECNOLOGÍA**

DIRECCIÓN DE POSTGRADOS

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL
TÍTULO DE MAGÍSTER EN GESTIÓN DE LA INFORMACIÓN E
INTELIGENCIA DE NEGOCIOS**

**INCIDENCIA DE LA INTELIGENCIA DE NEGOCIOS EN LA
CIBERSEGURIDAD, CON APLICACIÓN EN LAS POLÍTICAS
NACIONALES, CASO ECUADOR**

AUTOR: VACA HERRERA ANDREA ESTEFANÍA

DIRECTOR: RON EGAS MARIO BERNABÉ

**SANGOLQUÍ
2017**



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
MAESTRÍA EN GESTIÓN DE LA INFORMACIÓN E INTELIGENCIA DE
NEGOCIOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "INCIDENCIA DE LA INTELIGENCIA DE NEGOCIOS EN LA CIBERSEGURIDAD, CON APLICACIÓN EN LAS POLÍTICAS NACIONALES, CASO ECUADOR" realizado por la señorita Ing. **ANDREA ESTEFANÍA VACA HERRERA**, ha sido analizado por el software anti-plagio y revisado en su totalidad, determinándose que cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto autorizo para ser sustentado públicamente.

Sangolquí, 13 de junio del 2017

Ing. Mario B. Ron E. Mgs.

DIRECTOR DE TESIS



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
MAESTRÍA EN GESTIÓN DE LA INFORMACIÓN E INTELIGENCIA DE
NEGOCIOS

AUTORÍA DE RESPONSABILIDAD

Yo, ANDREA ESTEFANÍA VACA HERRERA, con cédula de identidad N° 1713643995, declaro que el trabajo de titulación: "INCIDENCIA DE LA INTELIGENCIA DE NEGOCIOS EN LA CIBERSEGURIDAD, CON APLICACIÓN EN LAS POLÍTICAS NACIONALES, CASO ECUADOR", ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros, que constan en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello soy responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 13 de junio del 2017

ANDREA ESTEFANÍA VACA HERRERA
C.C.1713643995

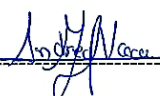


**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
MAESTRÍA EN GESTIÓN DE LA INFORMACIÓN E INTELIGENCIA DE
NEGOCIOS**

AUTORIZACIÓN

Yo, ANDREA ESTEFANÍA VACA HERRERA, autorizo a la Universidad de las Fuerzas Armadas ESPE, publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "INCIDENCIA DE LA INTELIGENCIA DE NEGOCIOS EN LA CIBERSEGURIDAD, CON APLICACIÓN EN LAS POLÍTICAS NACIONALES, CASO ECUADOR" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 13 de junio del 2017



ANDREA ESTEFANÍA VACA HERRERA

C.C.1713643995

DEDICATORIA

A Dios, por ser ese amigo indispensable, por estar cada día a mi lado apoyándome y diciendo “si se puede”, por darme esta oportunidad de crecer no solo como persona sino como una profesional. Dedico a mi amigo más fiel, que de un día para el otro se fue sin regresar, que me ayudó a no darme por vencida en ningún momento y desde el cielo me sigue dando ánimos para continuar con mis sueños y anhelos. También ofrezco este documento a mis padres, quienes con su consejo me ayudaron a establecer prioridades en la vida y vencer los obstáculos con tenacidad y valentía, a responsabilizarme por mis decisiones, que muchas veces fueron contrarias a lo que ellos deseaban, pero contando siempre con su apoyo incondicional.

Andrea Estefanía Vaca Herrera

AGRADECIMIENTO

Agradezco a Dios por su apoyo incondicional, por darme lo que más quiero en esta vida, mi familia y amigos, por no abandonarme y estar conmigo en los momentos difíciles de mi existencia. A mis padres por su gran paciencia, por ayudarme a ver la vida de una forma diferente, por los consejos que algunas veces solo los escuchaba y sufría por no seguirlos.

Para esas personas incondicionales que a pesar de que ya no están a mi lado, sé que desde el cielo me protegen y desean que me vaya bien tanto en lo personal como profesional.

Agradezco a mis amigos, que a pesar de la distancia me transmitieron su fuerza y voluntad para culminar una etapa más en mi vida, por ser incondicionales y pacientes.

Al Ingeniero Mario Ron quien aparte de ser mi profesor, ha sido un pilar que me ha sostenido y sigue guiando constantemente mi camino para alcanzar el éxito como persona y como profesional.

Andrea Estefanía Vaca Herrera

ÍNDICE DE CONTENIDOS

DEDICATORIA.....	v
AGRADECIMIENTO.....	vi
RESUMEN.....	xiv
ABSTRACT	xv
CAPITULO 1.- INTRODUCCIÓN	16
1.1. Justificación e Importancia	16
1.2. Planteamiento del problema	17
1.3. Formulación del problema a resolver.....	17
1.4. Hipótesis	18
1.5. Objetivos.....	18
CAPITULO 2.- MARCO TEÓRICO.....	20
2.1. Sistemas de Inteligencia de Negocios (BI) y su campo de Aplicación.-	20
2.2. Factores críticos de éxito para un sistema de Inteligencia de Negocios.....	25
2.3. Sistemas exploratorios de inteligencia de negocios cognitiva.-.....	26
2.4. La ciberseguridad y el manejo de grandes volúmenes de datos.....	28
2.5. Big Data en los entornos de defensa y seguridad	29
2.6. Ciberseguridad Inteligente, (Mosso, 2015)	31
2.7. Análisis de Big Data para la ciberseguridad, (T. Mahmood, 2013).....	33
2.8. Representación visual de patrones de ataque en ciberseguridad (Antonio, 2013)	35
2.9. Decisión Inteligente y Sistemas de Soporte para el diseño de políticas, (L. Niu, 2008).....	37
2.10. Estrategias Nacionales de Ciberseguridad (E. Leiva, 2015)	40
2.11. Políticas Nacionales de Ciberseguridad	41
2.12. Acerca de la soberanía del Ecuador en el ciberespacio.....	44
2.13. Métodos de Investigación de Campo.	45
2.14. El método Delphi.	45
CAPÍTULO 3.- METODOLOGÍA DE LA INVESTIGACIÓN.....	47
3.1- Objetivo Específico Nº 1.	47
3.2- Objetivo Específico Nº 2.	54
3.3- Objetivo Específico Nº 3.	60
3.4- Objetivo Específico Nº 4.	62

(Cisco, 2016)	65
3.5- Objetivo Específico N° 5.	66
CAPÍTULO 4.- PROPUESTA	75
4.1. Justificación de la Propuesta	75
4.2. Ejes de una Política Nacional de Ciberseguridad relacionada con BI.....	76
4.3. Funciones e institucionalidad necesarias para desarrollar una Política Nacional de Ciberseguridad relacionada con BI.	77
4.4. Esquema Gubernamental de Seguridad de la Información (EGSI).....	80
CAPÍTULO 5.- CONCLUSIONES Y RECOMENDACIONES.....	83
5.1. Conclusiones	83
5.2. Recomendaciones.....	84
BIBLIOGRAFÍA	85
ANEXOS.....	87
ANEXO A- ENCUESTA.....	87

ÍNDICE DE FIGURAS

Figura 1 Productos de Inteligencia de Negocios	21
Figura 2 Etapas del Modelo OID	24
Figura 3 Operaciones existentes en el Ciberespacio	32
Figura 4 Amenazas de los últimos años	34
Figura 5 Fases del Método Delphi	46
Figura 6 Resultados de la Pregunta 1	68
Figura 7 Resultados de la Pregunta 2	69
Figura 8 Resultados de la Pregunta 3	69
Figura 9 Resultados de la Pregunta 4	70
Figura 10 Resultados de la Pregunta 5	70
Figura 11 Resultados de la Pregunta 6	71
Figura 12 Resultados de la Pregunta 7	71
Figura 13 Resultados de la Pregunta 8	72
Figura 14 Resultados de la Pregunta 9	73
Figura 15 Resultado de la Pregunta 10	73
Figura 16 Funciones que la entidad debe cumplir	77
Figura 17 Entidades intervinientes	78

ÍNDICE DE TABLAS

Tabla 1 Amenazas.....	65
Tabla 2 Ejes de una Política de Ciberseguridad.....	76

GLOSARIO

Ciberseguridad.- Métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Ciberdefensa.- Aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques.

Inteligencia de Negocios.- Conjunto de estrategias, aplicaciones, datos, productos, tecnologías y arquitectura técnicas, enfocados a la administración y creación de conocimiento.

Big Data.- Macrodatos o datos masivos, hace referencia al almacenamiento de grandes cantidades de datos.

Patrones.- Modelo que sirve de muestra para obtener otra igual o compararla.

Estrategia.- Acción que se lleva a cabo para lograr un determinado fin.

Datawarehouse.- Colección de datos orientada a un determinado ámbito (empresa, organización).

Datamart.- Subconjuntos de datos que tienen el propósito de ayudar a un área específica del negocio, para que tome decisiones.

Legislación.- Conjunto de leyes por las cuales se regula un Estado o una actividad determinada.

Servicio.- Forma de proporcionar valor a los clientes facilitando los resultados que quieran alcanzar.

Impacto.- Categoría usada para identificar la importancia relativa de un incidente, un problema o un cambio. La prioridad se basa en el impacto y urgencia.

Victimas.- Personas u organizaciones que sufren un daño o perjuicio.

Ataque.- Método por el cual un individuo, mediante un sistema informático, intenta tomar su control.

Hacker.- Persona capaz de acceder o comprometer un sistema, robar o alterar su información.

Internet.- Conjunto descentralizado de redes de comunicación interconectadas.

Seguridad Informática.- Conjunto de métodos, normas y estándares que permiten asegurar que las políticas de una organización se cumplan.

Vulnerabilidad.- Punto débil del sistema que permite que un atacante comprometa la integridad, disponibilidad o confidencialidad de su información.

Delito Informático.- Toda acción tipificada, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Amenaza.- Aquello que potencialmente puede producir un daño en un sistema.

Acceso no autorizado.- Vulneración del acceso a un sistema utilizando medios no autorizados.

Red.- Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos.

Sistema Operativo.- Programa o conjunto de programas, que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación.

Contraseña.- Palabra secreta o una cadena de caracteres que son usados para la autenticación del usuario o para el acceso a un recurso.

Log.- Registro oficial de eventos durante un lapso de tiempo.

ACRÓNIMOS

BI	Business Intelligence
TI	Tecnologías de Información
ESPE	Escuela Politécnica del Ejército
TIC	Tecnologías de Información y la Comunicación
DNS	Domain Name System
ONU	Organización de las Naciones Unidas
OLAP	On Line Analytical Processing
OLTP	On Line Transactional Processing
CMI	Cuadro de Mando Integral
CMO	Cuadro de Mando Operativo
MIS	Management Information Systems
AIS	Administrative Information Systems
EIS	Executive Information Systems
GDSS	Group Decision Support Systems
DSS	Decision Support Systems
OID	Operation, Information and Decision
UIT	Unión Internacional de Telecomunicaciones
CMSI	Cumbre Mundial sobre la Sociedad de la Información
ETL	Extraction, Transformation and Load
Vs	Volúmen, Valor y Velocidad
IP	Internet Protocol
IEEE	Institute of Electrical and Electronics Engineers
SIEM	Security Information & Event Management
UPM	Universidad Politécnica de Madrid
ULACIT	Universidad Latinoamericana de Ciencia y Tecnología
INCIBE	Instituto Nacional de Ciberseguridad de España
COIP	Código Orgánico Integral Penal
PYME	Pequeña y Mediana Empresa
ISACA	Information Systems Audit and Control Association

RESUMEN

El desarrollo de nuevas tecnologías en los últimos años, ha sido de gran ayuda para todos los países, principalmente para los que se encuentran en vías de desarrollo; sin embargo, este avance ha provocado que la información no sea usada en forma adecuada, eficiente, eficaz y segura. Por esta razón es necesario establecer Políticas Nacionales de Ciberseguridad, en las que se incluya el apoyo de la Inteligencia de Negocios para filtrar grandes volúmenes de información y determinar patrones de comportamiento de la ciberdelincuencia que utiliza la tecnología para cometer cibercrímenes. Al momento no existe un estudio similar en el Ecuador, a pesar de la importancia que tiene el desarrollo, aprobación y aplicación de políticas de alto nivel que se traducen en normas y guías de orientación, que a su vez darán a luz proyectos que permita a las empresas e instituciones nacionales e internacionales radicadas en nuestro país, protegerse y actuar en contra de la ciberdelincuencia. El presente proyecto realizará el análisis del estado del arte relacionado con las metodologías, técnicas y herramientas de avanzada de Inteligencia de Negocios aplicadas a la ciberseguridad, así mismo la situación actual del Ecuador referente a este tema, su difusión, conocimiento y nivel de madurez, para en base de aquello proponer políticas innovadoras que se incluyan en el proyecto de Políticas Nacionales de Ciberseguridad. Será importante revisar los avances que al respecto tienen otros países del mundo y especialmente de la región y el nivel de penetración que tiene esta nueva tecnología en las empresas comerciales, industriales y financieras.

PALABRAS CLAVES:

- **INTELIGENCIA DE NEGOCIOS**
- **CIBERSEGURIDAD**
- **RIESGOS INFORMÁTICOS**
- **VULNERABILIDADES**
- **IMPACTO DE BI**

ABSTRACT

In the last years, new technologies are so important and helpful for all countries around the world, but the information is not using efficiently, and secure. For this reason, it is necessary to stablish National Cyber-Security Policies, which are integrate with Business Intelligence tools to filter big data and determine patrons to prevent cybercrimes. In Ecuador, there is not a study about it, in spite of the importance of information security. This research begins focusing on a systematic review about methodology, techniques and tools focus on Business Intelligence's actual situation, its trend and impact, it will continue with the local situation and a proposal of recommendations oriented to have a National Policy in Ecuador. It will be important to analyse Business Intelligence technology and compare with other countries to prevent new information attacks. Business Intelligence can be a good tool to analyse actual trends of Cyber Security and prevents bad uses of it. Business Intelligence is not only a subject to analyse company's situation, but also, can help to determine and prevent the next step to do a fraud in company's economy.

KEY WORDS:

- **BUSINESS INTELLIGENCE**
- **CYBERSECURITY**
- **INFORMATICS' RISKS**
- **VULNERABILITIES**
- **BI'S IMPACT**

CAPITULO 1.- INTRODUCCIÓN

Actualmente, las empresas manejan gran cantidad de información que puede ser usada de forma correcta o incorrecta, dependiendo de los usuarios y de las políticas de seguridad de la información que maneje la organización para brindar integridad, confidencialidad y disponibilidad a su información y confianza a sus clientes y relacionados.

La ciberseguridad (ISACA), es la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”. La información que se maneja hoy en día, se encuentra disponible en cualquier medio, debido a la conectividad de los dispositivos en la red.

La Inteligencia de Negocios ha sido utilizada para transformar los datos en información y la información en conocimiento, a través de un proceso sistemático y controlado; constituye también una estrategia, que permite aplicar métodos y técnicas para prevenir, detectar y minimizar ataques a los sistemas de información detectando patrones de comportamiento de los cibercriminales; éstas iniciativas se pueden ser tomadas como bases para una propuesta de nuevas políticas a nivel de país, referidas a la seguridad de la información. La protección de la información y la toma de decisiones en las empresas son aspectos muy importantes y por tanto la fusión de sus métodos y técnicas de trabajo puede generar políticas que ayuden al país a proteger la información, especialmente aquella que se procesa en grandes volúmenes producto de la alta transaccionalidad de las operaciones de negocios o financieras.

1.1. Justificación e Importancia

La gran cantidad de información que hoy se maneja en diversos ambientes, se transmite en por la red sin que sus usuarios o administradores tengan una plena conciencia de que muchas veces puede ser interceptada para fines maliciosos.

La toma de decisiones en una empresa es fundamental, por esa razón la información pertinente deberá conservar sus atributos de confidencialidad, integridad y disponibilidad, sumada al gran volumen y grado de abstracción con que se utiliza la información procesada.

La ciberdelincuencia utiliza procedimientos masivos de intrusión y técnicas comunes que pueden detectarse en base de un patrón de comportamiento o procedimiento digital, que puede ser descubierto con Minería de datos u otras técnicas de filtrado de Big Data, minimizando el tiempo de retardo en el procesamiento de la información y la disponibilidad de la misma.

Las infraestructuras críticas nacionales, especialmente aquellas relacionadas con los servicios financieros, pueden ser afectadas si no se cuenta con políticas de inteligencia de negocios aplicadas a la ciberseguridad. Es por esta razón que los países industrializados han puesto énfasis en el desarrollo de políticas, las que a su vez han permitido el desarrollo de la tecnología relacionada que sirve para el filtrado de software malicioso, detección de intentos de intrusión, IDS, IPS, SIEM y otros instrumentos técnicos de protección de los activos de información de las empresas.

1.2. Planteamiento del problema

Grandes volúmenes de datos son transmitidos desde fuera de las fronteras de un país y así mismo cantidades similares son transmitidos y procesados internamente; entre esta inmensa cantidad de datos, se encuentran aquellos que representan un gran riesgo de seguridad a la nación y sus conciudadanos, especialmente en el funcionamiento de las infraestructuras críticas que son vitales para el desarrollo del país y su supervivencia como nación.

Las amenazas escondidas o camufladas entre estos datos, no son fáciles de detectar con medios convencionales, la determinación de comportamientos inusuales tampoco puede hacerse de manera rápida y certera. La detección y en consecuencia el tiempo de reacción para impedir o minimizar el impacto del cibercrimen es crítico y cada vez se hace más corto si se quiere mantener la integridad, confidencialidad y disponibilidad de la información que está ligada a un entorno físico real.

No existen al momento en el Ecuador, sistemas y métodos de defensa y seguridad cibernéticos definidos desde una estrategia que sea desarrollada en varios niveles de abstracción, con una estructura coherente para actuar de manera sistemática en contra de estas amenazas.

1.3. Formulación del problema a resolver

- ¿Se conoce en forma sistematizada la situación actual del país, en relación al uso de metodologías y herramientas que permitan asegurar la integridad,

confidencialidad y disponibilidad de grandes volúmenes de datos que son transmitidos desde fuera de las fronteras de un país y así mismo los que son transmitidos y procesados internamente, para permitir el funcionamiento de las infraestructuras críticas que son vitales para el desarrollo del país y su supervivencia como nación?

- ¿Cuáles son las amenazas que pueden ser escondidas o camufladas entre grandes volúmenes de datos, que no sean fáciles de detectar con medios convencionales?
- ¿Cómo se puede determinar los comportamientos inusuales en el ciberespacio en grandes volúmenes de datos, de manera rápida y certera?
- ¿Qué sistemas y métodos de defensa y seguridad cibernéticos pueden ser definidos en el Ecuador, partiendo de estrategias y políticas desarrolladas en varios niveles de abstracción, con una estructura coherente para actuar de manera sistemática en contra de las amenazas cibernéticas?

1.4. Hipótesis

Es posible definir para el Ecuador, sistemas y métodos de defensa y seguridad cibernéticos que utilicen Inteligencia de Negocios, para establecer estrategias y políticas nacionales que se desarrollen en varios niveles de abstracción, con una estructura coherente para actuar de manera sistemática en contra de las amenazas cibernéticas, habiendo conocido la situación actual del país, en relación al uso de metodologías y herramientas que permitan asegurar la integridad, confidencialidad y disponibilidad de grandes volúmenes de datos que son transmitidos desde fuera de las fronteras de un país y así mismo los que son transmitidos y procesados internamente, para permitir el funcionamiento de las infraestructuras críticas que son vitales para el desarrollo del país y su supervivencia como nación; habiendo definido también las amenazas que pueden ser escondidas o camufladas entre grandes volúmenes de datos, que no sean fáciles de detectar con medios convencionales, determinando los comportamientos inusuales en el ciberespacio.

1.5. Objetivos

1.5.1. Objetivo General

Realizar un análisis sistemático y una investigación de campo para definir para el Ecuador, sistemas y métodos de defensa y seguridad cibernéticos que utilicen Inteligencia de Negocios, establecer estrategias y políticas nacionales que se desarrollen en varios niveles de abstracción, con una estructura coherente que permita actuar de manera sistemática en contra de las amenazas cibernéticas que pueden ser escondidas o camufladas entre grandes volúmenes de datos, que no sean fáciles de detectar con medios convencionales, determinando los comportamientos inusuales en el ciberespacio de manera rápida y certera.

1.5.2. Objetivos Específicos

- Investigar en forma sistematizada la situación actual del país, en relación al uso de metodologías y herramientas que permitan asegurar la integridad, confidencialidad y disponibilidad de grandes volúmenes de datos que son transmitidos desde fuera de las fronteras de un país y los que son transmitidos y procesados internamente, para permitir el funcionamiento de las infraestructuras críticas que son vitales para el desarrollo del país y su supervivencia como nación.
- Determinar las amenazas que pueden ser escondidas o camufladas entre grandes volúmenes de datos, que no sean fáciles de detectar con medios convencionales.
- Establecer la forma en la que se puede determinar los comportamientos inusuales en el ciberespacio en grandes volúmenes de datos, de manera rápida y certera.
- Establecer los sistemas y métodos de defensa y seguridad cibernéticos que pueden ser definidos en el Ecuador, partiendo de estrategias y políticas desarrolladas en varios niveles de abstracción, con una estructura coherente para actuar de manera sistemática en contra de las amenazas cibernéticas.
- Elaborar una propuesta para el Ecuador, sistemas y métodos de defensa y seguridad cibernéticos que utilicen Inteligencia de Negocios, para establecer estrategias y políticas nacionales que se desarrollen en varios niveles de abstracción, con una estructura coherente para actuar de manera sistemática en contra de las amenazas cibernéticas que pueden ser escondidas o camufladas entre grandes volúmenes de datos, que no sean fáciles de detectar con medios convencionales, determinando los comportamientos inusuales en el ciberespacio de manera rápida y certera.
- Verificar la validez de la propuesta mediante evaluación de expertos.

CAPITULO 2.- MARCO TEÓRICO

2.1. Sistemas de Inteligencia de Negocios (BI) y su campo de Aplicación.-

El activo más importante de una empresa es la información que se encuentra almacenada en sus propias bases de datos. Sin embargo, su uso no es eficiente y muchas veces no es el correcto, porque los empresarios la gestionan de mala manera o no utilizan un procesamiento adecuado. Actualmente, la tecnología cuenta con nuevas herramientas que permiten reducir costos y tiempo en el procesamiento de la información para presentar información útil para la toma de decisiones en el negocio.

Aquí, es donde la Inteligencia de Negocios toma lugar, para permitir una visión estratégica, reducir el riesgo y la incertidumbre en la toma de decisiones empresariales y construir ventajas competitivas a corto y largo plazo.

Los Sistemas de Inteligencia de Negocios son un conjunto de componentes que permiten la toma de decisiones a partir del procesamiento de la información y pueden ser:

- **DataMart:** es una base de datos departamental, especializada en el almacenamiento de los datos de un área de negocio específica. Se caracteriza por disponer de la estructura óptima de datos para analizar la información al detalle desde todas las perspectivas que afecten a los procesos de un departamento. Se habla de dos tipos de DataMart (L. JIMENEZ)
 - Datamart OLAP: se basa en los cubos OLAP (Online Analytical Processing) que se construyen agregando las dimensiones e indicadores necesarios de cada cubo relacional.
 - Datamart OLTP: es la introducción de mejoras en el rendimiento, como agregaciones y los filtrados.
- **DataWarehouse:** es una base de datos corporativa que se caracteriza por integrar y depurar información de una o más fuentes distintas, para luego procesarla permitiendo su análisis desde infinidad de perspectivas y con grandes velocidades de respuesta. Según definió el propio Bill Inmon, un datawarehouse se caracteriza por ser:

- Integrado: debe haber información consistente, todos los datos almacenados deben ser integrados en una estructura sin inconsistencias.
- Temático: los datos deben ser los necesarios, es decir, que debe estar la información que se necesita. Así la información será la que el cliente necesite y facilitará a consultas.
- Histórico: tener históricos de la información permite analizar las tendencias de un negocio, ayudando así a la toma de decisiones por la comparación de información.
- No Volátil: la información de un datawarehouse, es información que permanece y que el usuario pueda leer pero no modificarlo.

La Inteligencia de Negocios es un conjunto de herramientas y aplicaciones, que permite procesar la información y ayudar a los empresarios en la toma de decisiones. Para ello la Inteligencia de Negocios posee los siguientes productos. Ver Figura 1.

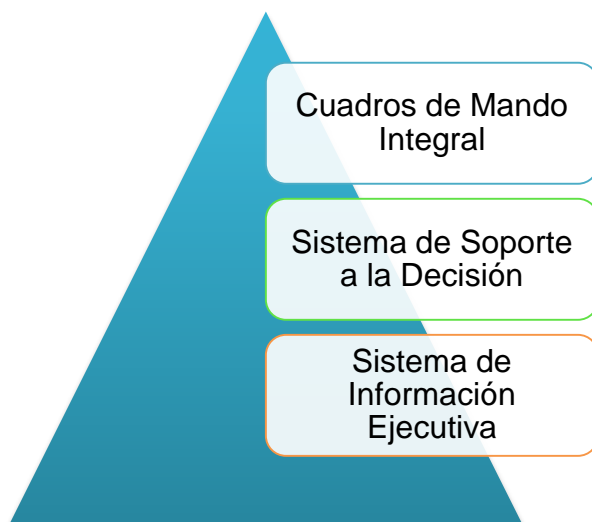


Figura 1 Productos de Inteligencia de Negocios

- **Cuadro de Mando Integral (CMI):** también conocido como Balanced Scorecard (BSC) o dashboard, es una herramienta de control empresarial que permite establecer y monitorear los objetivos establecidos de una organización y de sus áreas. Gracias a esta herramienta se puede ver el cumplimiento de estrategias de acuerdo a los objetivos establecidos, conocer las tareas cumplidas/por cumplir y las personas que se encuentran asignadas a ellas. Es de dos tipos:

- Cuadro de Mando Operativo (CMO), es una herramienta de control que se enfoca en el seguimiento de variables operativas.
- Cuadro de Mando Integral (CMI) representa la ejecución de la estrategia de una compañía desde el punto de vista de la Dirección General.
- **Sistema de Soporte a la Decisión:** es una herramienta enfocada al análisis de los datos de una organización, permitiendo la integración de todos los sistemas o departamentos de una organización. Los sistemas de Soporte de Decisión son de tres tipos:
 - Sistemas de información gerencial (MIS): también llamados Sistemas de Información Administrativa (AIS), brinda soporte a trabajos organizacionales.
 - Sistemas de información ejecutiva (EIS): contiene información más sencilla y accesible a los altos mandos de una organización.
 - Sistemas expertos basados en inteligencia artificial (SSEE): son llamados también sistemas basados en conocimiento, utilizan redes neuronales para hacer una simulación del conocimiento de un experto que lo usan para resolver problemas.
 - Sistemas de apoyo a decisiones de grupo (GDSS): son sistemas basados en equipos computacionales que apoyan a grupos de personas que tienen un objetivo en equipo y que sirve como interfaz con un ambiente compartido.
- **Sistema de Información Ejecutiva:** es una herramienta de software, basada en un DSS, que suministra a los gerentes un fácil acceso a la información interna y externa de su compañía. Su función es que el ejecutivo tenga un panorama completo de la empresa en tiempo real, manteniendo la posibilidad de observar con detalle aquellos que no estén llegando a las expectativas establecidas, para determinar el con detalle aquellos que no estén llegando a las expectativas establecidas, para determinar el no estén (S. BARRENTO, 2010))

La inteligencia de negocios puede ser aplicado a los siguientes fines comerciales, con el objetivo de impulsar el valor del negocio:

- **Gestión del Conocimiento:** permite generar conocimiento para el manejo del aprendizaje y cumplimiento normativo de la empresa.

- **Plataforma de colaboración:** obtiene diferente información de varias áreas a través del intercambio de datos entre las mismas.
- **Informes o reportes:** permite la visualización de información de una forma más dinámica o entendible para un usuario final.
- **Analítica:** constituyen procesos cuantitativos para ayudar a la toma de decisiones óptimas. Se aplica la minería de datos, minería de procesos, análisis estadístico, entre otros.
- **Medición:** permite la creación de jerarquía de medidas de rendimiento, usadas básicamente para realizar un enfoque a los empresarios del estado de su empresa.

Un sistema de Inteligencia de Negocios, se basa en una arquitectura construida a través de un Modelo OID de tres subsistemas: sistema de Operación, sistema de Información y sistema de Decisión. (L. Jimenez). Esta arquitectura, básicamente, se basa en cuatro capas: la primera capa: fuente de datos, en donde se encuentran todos los datos operacionales que maneja una empresa. La siguiente capa es el proceso de extracción y transformación de datos, en la que se puede usar varias herramientas, sin embargo depende de la integridad de datos que se recolecta en la primera capa, que es una de las más críticas y difíciles de tratar. La siguiente capa son los almacenes, llamados datawarehouse, en la que básicamente, se habla de los hechos y sus dimensiones y finalmente, la última capa, Inteligencia de Negocio, representa la lógica del negocio que responde a las preguntas que los grandes mandos necesitan para que su empresa se encuentre en el mercado. A continuación se puede observar las cuatro etapas de la Inteligencia de Negocios, en la Figura 2 Etapas del Modelo OID.

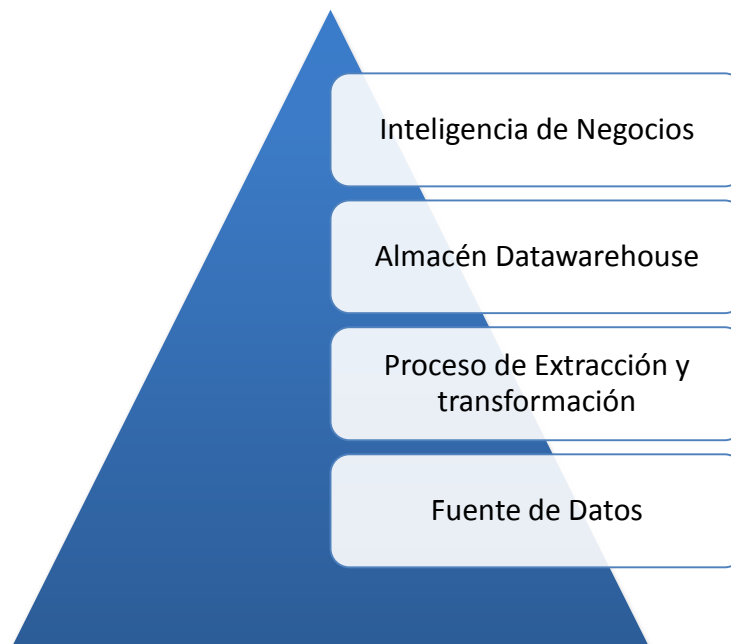


Figura 2 Etapas del Modelo OID

La metodología de un sistema de Inteligencia de negocio se divide en cuatro etapas: Planeamiento, requerimientos y análisis del negocio, diseño y construcción, (L. Jimenez)

- Planeamiento: maneja el plan del proyecto de implementación de un sistema de inteligencia de negocio, tomando en cuenta los tiempos y los recursos que se va a utilizar.
- Requerimientos y análisis del negocio: se refiere a los detalles específicos y generales del negocio de una empresa, que hace la empresa, en qué está enfocada y sus limitaciones.
- Diseño: estructura los datos recogidos de cada área y realiza un bosquejo de cómo se va a ejecutar el modelo de negocios del sistema.
- Construcción: es la implementación del sistema de inteligencia de negocios de acuerdo a los requerimientos y análisis realizado anteriormente. Utilizando los siguientes subprocesos:
 - Extracción: se recobra datos a partir de las fuentes de datos, es decir, datos operacionales.
 - Limpieza: ayuda a la comprobación de la integridad de los datos que se obtuvo en la etapa anterior, se modifica los errores y se completa los datos vacíos.
 - Transformación: se basa en recolectar datos consistentes, útiles y de calidad.

- Integración: este proceso se basa en una validación de datos, comprobando la consistencia de las definiciones de los formatos de los datawarehouse definidos en el modelo conceptual de la empresa.
- Actualización: permite actualizar los datos de cada uno de los datawarehouse que se conformen en la empresa.

2.2. Factores críticos de éxito para un sistema de Inteligencia de Negocios

Una investigación realizada por dos estudiantes de una universidad de Australia, define a un sistema de Inteligencia de negocio como un conjunto de herramientas integradas que recogen, integran, analizan y hacen que la información sea confiable para el usuario final. A pesar de que la Inteligencia de Negocios es un concepto que no se ha estudiado mucho en los últimos años debido a su aparición reciente, existen muchas interacciones con el uso de grandes cantidades de datos que permiten el análisis y la gestión de nuevo conocimiento usando esos datos para la toma de decisiones. Las empresas analizan, integran y crean nuevo conocimiento con los sistemas de Inteligencia de negocios.

Un sistema de Inteligencia de Negocio, no solo recibe datos duplicados, puede recibir datos vacíos e irrelevantes para un usuario final, por esta razón, un sistema de inteligencia de negocio es una solución integral que abarca varias herramientas, donde recoge toda la información posible (datos vacíos, duplicados e inútiles), luego los analiza y transforma en datos legibles que el usuario necesita conocer. Después de la transformación, esos datos se correlacionan con la información que se encuentra disponible y empieza a generar nuevo conocimiento que se presentará en varios esquemas de visualización de información como Histogramas, pasteles, entre otros, haciendo la información legible para el usuario final.

Para la creación de un sistema de inteligencia de negocios, se usa varios casos de estudio para obtener sus factores críticos de éxito. El análisis de los casos de estudio permite hacer un análisis de las empresas en donde fueron (R. Wetzker, 2007) implementados con anterioridad y como las ayudaron en la toma de decisiones. Su negocio y el giro de negocio se basan en la toma de decisiones de corto y largo plazo. En conclusión, los sistemas de inteligencia de negocios, no solo integran sistemas externos, sino que crean nuevos sistemas que permiten analizar datos y transmitirlos con información útil. (W. Yeoh, 2010)

2.3. Sistemas exploratorios de inteligencia de negocios cognitiva.-

Básicamente son sistemas tradicionales de inteligencia de negocios que permiten la toma de decisiones desde los aspectos cognitivos del ser humano. Es un proceso mediante el cual se manipula grandes volúmenes de información de una compañía, su objetivo es tomar decisiones a través del modelo cognitivo de un ser humano, usando modelos mentales para tomar mejores decisiones. Se basa en la situación de la conciencia que es un concepto cognitivo de la psicología donde existe tres niveles: Percepción, entendimiento de la información y por último predicción de acuerdo al comportamiento de las personas en el ambiente o entorno que se encuentran.

El uso de los modelos mentales permite al ser humano explicar cómo funciona el mundo real, permite así el uso de varios conceptos y la generación de nuevo conocimiento para tomar decisiones. Presenta su propia arquitectura dividida en cuatro capas:

- Capa Ejecutiva: se centra básicamente en la retroalimentación de los sistemas computacionales, integra los modelos mentales y el concepto psicológico, se la llama situación de conciencia o parte cognitiva.
- Capa de Soporte de Pensamiento: provee a la capa ejecutiva un conjunto de herramientas para la gestión de conocimiento y el proceso de pensamiento, tiene cinco sub-módulos:
 - Caso-base: es el conocimiento explícito de un problema resuelto, puede ser individual o grupal.
 - Base del modelo mental: es una representación de la construcción mental del ser humano, utiliza la técnica de mateo cognitiva, donde se usa conceptos de nodos y relaciones, refleja así los conceptos que una persona tenga para describir cómo funciona el mundo.
 - Gestión de casos/ modelos mentales: este sub-módulo representa, carga, actualiza y elimina modelos/ casos mentales.
 - Agente del conocimiento: recibe todas las peticiones de la capa de base del modelo mental y analiza ese conocimiento, creando así un nuevo conocimiento.
- Capa de Situación de la Evaluación: ayuda al ejecutivo a tomar las decisiones de la empresa.

Está constituido por tres sub-módulos:

- SA Agente: recibe las entradas del módulo anterior y las peticiones de conocimiento del módulo de soporte de pensamiento. son básicamente archivos XML multidimensionales, los que serán analizados para poder generar nuevo conocimiento.
 - Situación de búsqueda: permite la búsqueda de información relevante para la actual toma de decisiones
 - Situación de representación: permite presentar los datos procesados al usuario final, es el nuevo conocimiento que faculta ver los avances de una empresa. Esta información se la representa en histogramas, gráficos. entre otros.
- Subsistema Datawarehouse, está conformado por sistemas operacionales, adquisición de datos, almacenamiento de información y el análisis de los datos que recibe de las fases anteriores.

La propuesta de esta investigación es importante debido al uso de simples y comunes sistemas de inteligencia de negocios mezclado con el concepto de cognitivo, es decir, el uso de mapas mentales de los seres humanos para tomar decisiones, es la integración de varias herramientas para la recolección, el almacenamiento, discriminación de datos y por último la creación de nueva información para la presentación de datos a un usuario final. La combinación entre varios sistemas permite a un usuario final obtener información más acertada y que ayude a distinguir varias opciones de invertir o no en un negocio. La tecnología trata de hacer que las computadoras actúen como un ser humano, es decir, realizar sistemas inteligentes donde se ahorre tiempo y se reciba ganancias por ese ahorro, los sistemas de negocio, en su parte, permite que una persona sea más competitiva en el mercado, creando estrategias en varias aéreas y planeando nuevos retos, gracias al análisis de datos que realizan.

Los sistemas cognitivos de inteligencia de negocios, permiten involucrar nuevas técnicas y herramientas como los mapas mentales, permitiendo involucrar al ser humano con los sistemas computacionales y realizar nuevo conocimiento presentando información legible. (R. Wetzker, 2007)

2.4. La ciberseguridad y el manejo de grandes volúmenes de datos.

La ciberseguridad es un término que muchas de las empresas lo tienen en el olvido, por el simple hecho que no han tenido ningún percance con su información. Sin embargo, el hecho no haber sido víctimas de un ataque cibernético, no quiere decir que todo el tiempo será así. Hoy en día existen más posibilidades de que cualquier persona tenga acceso a la información de una organización.

Ciberseguridad se la conoce como el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en toda la organización.

Big data es un término aplicado a conjuntos de datos que superan la capacidad del software habitual para ser capturados, gestionados y procesados en un tiempo razonable. La enorme cantidad de información produce bloqueo: a más cantidad de datos, menor capacidad de toma de decisiones adecuadas.

El manejo de grandes cantidades de información, hace que las empresas se despreocupen de su seguridad, esto se debe a que muchas veces están enfocados en el proceso de la información para la generación de nuevo conocimiento y toma decisiones.

La ciberseguridad y el manejo de grandes volúmenes de información, hoy en día, deberían ser dos conceptos que vayan de la mano, debido a que la información debe ser siempre confidencial, íntegra y disponible, la información debe tratarse con más cuidado por la clase de datos que se transmite a los usuarios y cómo estos datos están siendo utilizados por las empresas.

La Ciber Estrategia Militar pretende obtener superioridad en la guerra cibernética, la investigación realizada por el Departamento de Milicia de la Universidad de Daejeon de la República de Corea, se enfocan en los diversos ataques cibernéticos que hoy en día la información es propensa en especialmente la relacionada con la milicia. Dependiendo del negocio o de las funciones de una empresa, pueden existir varias estrategias de seguridad para el ciberespacio, se puede observar los posibles ataques y como estos podrían ser bloqueados para que la información se mantenga segura. En la investigación coreana, se demuestra que el ciber espacio posee una infraestructura de tres capas: Cibernética, de Infraestructura Crítica / Recursos Claves

y la de Infraestructura física. Considerando estas capas se propone estrategias cibernéticas militares importantes para controlar la seguridad de grandes volúmenes de información que controla la milicia. El uso de estas estrategias hace que la empresa controle o tenga un poder importante de sus recursos y así pueda asegurar su información. Al manejar grandes volúmenes de información, muchas de las veces, se toman datos que no son útiles para el usuario final, por lo que se debe considerar ciertos aspectos para el manejo de estos datos, sin olvidar su seguridad. Es por esa razón que al manejar grandes volúmenes de datos en el área militar, se enfocan en la estructura del ciberespacio para determinar las estrategias que permitan brindar seguridad a ése volumen de datos. (J. Eom, 2012)

En el artículo técnico: Revisión Sistemática de Literatura: Visualización de Seguridad, se habla de las diferentes visualizaciones de la información, tipos de fuentes de datos, lenguajes de programación y los ataques que se realizan a estos. Lo más complicado para las empresas es mantener su información íntegra, debido a las nuevas tecnologías que permiten a las personas conocer su información para fines maliciosos. En esta investigación se realiza un estudio de la presentación de la información. Los datos de una empresa pueden ser representados en diversas formas como Histogramas, pasteles, barras, entre otros, este tipo de visualización pueden ser representadas en tiempo real o simplemente por periodos. Los ataques más comunes para cada uno de estas visualizaciones de información son: Denegación de servicio, escaneo de puertos, propagación de malware, entre otros. Gracias al uso de Inteligencia de Negocios, se puede usar patrones que permitan determinar los diferentes ataques que una empresa puede estar propensa al presentar sus datos en las visualizaciones de información descritas anteriormente. Adicionalmente, con los patrones se puede prevenir el control de los puertos usados por las personas en una empresa y establecer estrategias de seguridad de la información, de acuerdo a las reglas de negocio de la organización. En conclusión, la combinación de la ciberseguridad y el manejo de grandes volúmenes de información, hace que una empresa sea fuerte en el campo de seguridad. (G. Mondrag)

2.5. Big Data en los entornos de defensa y seguridad

Es una investigación basada en el estudio de Big Data o también conocida como las cuatro Vs: Volumen, Valor, Velocidad y Variabilidad de la información. El uso de

grandes cantidades de información, hoy en día, es un tema que ha generado grandes avances en la empresa debido a la generación de conocimiento en grandes volúmenes, variabilidad y velocidad con la que es procesada la información. Sin embargo, los valores de los datos muchas veces no son como se originaron por lo que implica otro estudio y otro proceso especial debido al gran volumen de información. No todos los datos que se manejan pueden ser útiles o no todos los datos son verídicos, porque pudieron ser atacados o alterados por personas internas o externas a una empresa.

Existen varios conceptos de Big Data, pero en resumen es el manejo de grandes cantidades de información a una velocidad diferente y que pueden variar dependiendo la velocidad de operación. Antes se podría decir que existían pocas empresas que manejen Big Data, ahora, la mayoría de empresas que manejan datos estructurados y no estructurados lo hacen. La información es cada vez más grande debido a las transacciones o peticiones que manejan las empresas. La tendencia es que todo vaya a la nube pensando en un ahorro para la empresa, pero se pierde en seguridad de la información. Esta investigación aplica conceptos de seguridad y defensa de la información, considerando que la información en grandes cantidades no puede tener el mismo tratamiento que una información normal, se puede perder datos importantes o manejar datos inútiles para el usuario, por tanto, para el análisis o gestión de grandes volúmenes de información se usa varias herramientas o soluciones que tienen vulnerabilidades y pueden estar propensas a recibir ataques. El uso de Big Data, puede estar orientado a los siguientes ámbitos:

- Detección de intrusión física en grandes espacios o infraestructuras abiertas
- Computación sobre información encriptada
- Análisis automático de vulnerabilidades de red (máquinas-tráfico de datos)
- Criminología computacional
- Uso fraudulento de recursos corporativos y/o sensibles
- Análisis de video en tiempo real / Búsqueda y recuperación rápida en librerías de video.
- Inteligencia visual en máquinas
- Identificación de anomalías, patrones y comportamiento en grandes volúmenes de datos.

- Análisis de texto (estructurado y no estructurado) como apoyo a la toma de decisión en tiempo real en entornos intensivos en datos.
- Conciencia situacional
- Traducción automática a gran escala (en número de idiomas y en volumen)
- Predicción de eventos

Una de las aplicaciones más importante de Big Data es en la Ciberseguridad, debido al tratamiento de la información que le proporciona usando las técnicas de análisis y de gestión de conocimiento le permite conocer los ataques más variados que en la actualidad se tenga y como prevenirlos. Al usar Big Data en grandes volúmenes de información permite determinar varios ataques que son muy comunes en la actualidad y prevenir que esos ataques ocasionen caídas de los sistemas de una empresa. El uso de varios puertos para cierta información, también puede dar apertura a la contaminación del resto de información, por lo que el bloqueo de los puertos pueden ser una alternativa o parte de las estrategias de ciberseguridad que deben ser implementadas en una empresa. (J. Carrillo Ruiz, 2013)

2.6. Ciberseguridad Inteligente, (Mosso, 2015)

Esta investigación se enfoca en una alternativa para proteger la información de las empresas, cuyos los modelos de negocio toman información importante del ciberespacio y por tanto se encuentran expuestas a los ataques y son muy vulnerables a ellos. La investigación propone realizar ciberseguridad inteligente para proteger la información de un negocio que se encuentra en la nube o simplemente que comparten con otras empresas, es decir, que se mantienen conectadas entre sí y usan una infraestructura que incrementa la probabilidad de que sus datos sean intervenidos por otras personas y sea usada la información para fines maliciosos, pero las organizaciones, a pesar de que se encuentran preocupados por este problema, muchas de las veces la seguridad la consideran un gasto en lugar de una inversión.

El ciberespacio, es un lugar donde se comunican personas, software y servicios a través del Internet sin figuras físicas ni equipos. Existen varios blancos en el ciberespacio de acuerdo al tipo de amenaza:

- Estados Nación: la capacidad de acceso es más propensa a amenazas por el tipo de acceso que maneja. Esto se debe a la contratación de terceros donde se puede atacar recursos.

- Grupos Organizados Transnacionales: son grupos externos que pueden realizar fraudes o cualquier actividad ilícita perjudicando no solo a una empresa sino a nivel nación o nivel país.
- Pequeños grupos o individuos: es una amenaza menor que las anteriores, pero así mismo perjudicial, se refiere a la interrupción de los servicios de una empresa.
- Amenaza interna: es una amenaza por las personas internas de la empresa que poseen accesos y quieren perjudicar a una empresa.

Después del análisis de las amenazas se estudia los tipos de operaciones que existen en el ciberespacio y las divide en tres:

- Operaciones ofensivas: acciones contra potenciales adversarios y agentes maliciosos que afectan a la integridad y disponibilidad de los sistemas de información.
- Operaciones defensivas: conjunto de medidas y acciones encaminadas a detectar, identificar, interceptar, rechazar y neutralizar todo tipo de ataques o intentos de penetración
- Operaciones de inteligencia: acciones destinadas a generar nuevos conocimientos para evitar cualquier tipo de amenaza.



Figura 3 Operaciones existentes en el Ciberespacio

También, se habla de un concepto llamado inteligencia del ciberespacio (CIBERINTEL), disciplina que recibe varios insumos y genera nuevos. Permite que los usuarios tengan conciencia de las amenazas que su información esta propensa a tener.

La ciberseguridad inteligente es un complemento de las capacidades de protección del ciberespacio, consta de tres niveles:

- Nivel táctico del ciberconflicto: es un nivel donde existe una planificación, y la ejecución de esa planificación contra la persona que está realizando el ataque.
- Nivel operacional del ciberconflicto: planificación, conducción y mantenimiento de las estrategias operacionales de una empresa en la ciberseguridad. Básicamente el uso de herramientas para la detección de amenazas.
- Nivel estratégico del ciberconflicto: en este nivel se establece las estrategias de la empresa con respecto a la ciberseguridad de su información, usando los recursos que posee para su ejecución. Este es el nivel superior en donde los altos mandos ejecutan sus decisiones.

En conclusión, esta investigación está basada en un estudio de las amenazas a las que se encuentra expuesta la información por encontrarse en el ciberespacio, sin embargo, las autoridades especialmente se encuentran preocupadas por la información que se transmite por la internet sin que se brinde la seguridad adecuada, por eso es importante analizar las amenazas y tomar acciones al respecto. La información es un activo muy importante en una empresa, por lo que se hace necesario establecer políticas de seguridad a nivel gerencial y a nivel nacional.

2.7. Análisis de Big Data para la ciberseguridad, (T. Mahmood, 2013)

Esta investigación se refiere a la nueva era de Big Data y la seguridad de la información. El arte del análisis de la seguridad permite a los investigadores conocer los sistemas que se encuentra en cada empresa y conocer las vulnerabilidades que ellas tienen. La información se encuentra en constante cambio y modificación al circular por la red de la empresa y en otras partes del mundo a través del uso de Internet, por lo que un análisis de la red y de la seguridad que se maneja permite que la empresa conozca las vulnerabilidades y amenazas en tiempo real.

El internet maneja mucha información de todas las partes del mundo y se constituye una puerta abierta para los ataques cibernéticos. De acuerdo al estudio éstos son los más comunes en los últimos días:

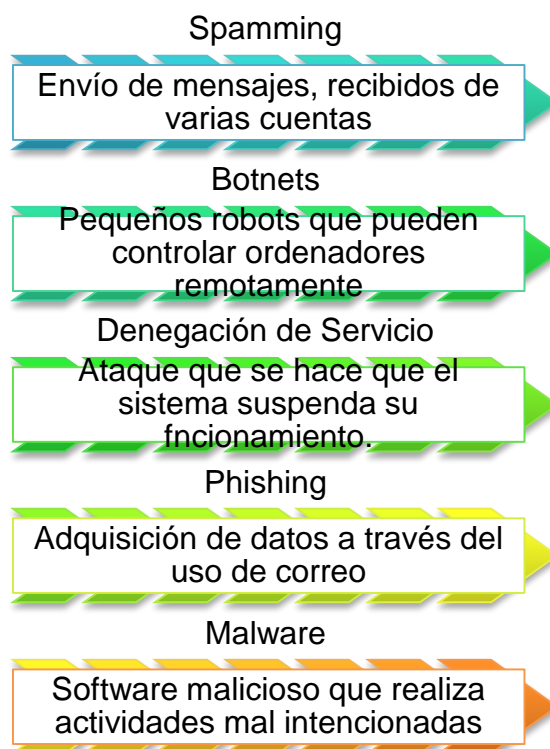


Figura 4 Amenazas de los últimos años

Los principales objetivos de la ciberseguridad se determinan como:

- Obtener y compartir información de forma segura para la toma de decisiones precisa,
- Encontrar y hacer frente a las vulnerabilidades dentro de las aplicaciones,
- Evitar el acceso no autorizado
- Proteger la información confidencial

Estos objetivos, en cierta manera, se puede cumplir usando herramientas o soluciones de seguridad, sin embargo, con Big data y el uso de grandes volúmenes de información ha sido un poco más complejo proveer seguridad, debido al acceso a la información, porque es más vulnerable de ser atacada considerando que la información no solo se encuentra en la empresa sino fuera de ella. Adicionalmente, al manejar grandes volúmenes de información, se hace más complejo su análisis y revisión debido a las diferentes fuentes de datos de donde se la obtiene, así también

puede estar almacenada en diferentes partes sin que se conozca la infraestructura ni las vulnerabilidades que estas pueda tener. Por esta razón, se hace necesario la investigación del proceso de análisis de Big Data, para determinar las aplicaciones idóneas que puedan brindar un procesamiento seguro de grandes volúmenes de datos. Para el análisis de Big Data se considera la siguiente secuencia:

- Análisis y selección de la información en tiempo real
- Pre-procesamiento de la información, es decir, limpiarla, que no exista datos duplicados, datos vacíos, normalizados. Este proceso se lo conoce como ETL (Extract, transform, Load)
- Una vez limpia la información se realiza el almacenamiento y análisis de la importancia de cada dato para ser presentada con varias técnicas de visualización de información.

Luego de determinar el proceso para manejar grandes volúmenes de información, los investigadores proponen un modelo de análisis de seguridad caracterizado por diversas fuentes de datos, herramientas de ETL, motores de análisis de Big Data y sistemas de monitoreo. El modelo permite analizar las vulnerabilidades que la información puede presentar. En conclusión, se propone analizar los datos que se recibe de varias fuentes de datos usando varias herramientas, algunas pagadas y otras libres, luego analizar los datos, que estos se encuentren libres de duplicaciones, y alteraciones para ser almacenados y presentados a un usuario o cliente final a fin de que tome decisiones.

2.8. Representación visual de patrones de ataque en ciberseguridad (Antonio, 2013)

Se realiza la investigación referida a la enorme cantidad de ataques que sufre la información debido a la interconectividad de las personas y del mundo. Por esta razón, el análisis de datos, procesamiento y análisis de la información a través de patrones, ayudará para el fácil descubrimiento y prevención de ataques.

El uso de Big Data, con grandes volúmenes de datos, el análisis y la correlación entre ellos, permite el diseño de patrones que pueden convertirse en conocimiento para las empresas y ayuda en la toma de decisiones. El objetivo de la investigación es diseñar una herramienta que permita la recolección de datos, su análisis y su gestión para que sea transformada en conocimiento y permita a las empresas

construir patrones para tomar las mejores decisiones de seguridad en sus empresas y cuidar la información que manejan.

Lo más importante de la empresa son los datos que se recibe al iniciar cualquier proceso, los datos deben ser los necesarios y precisos, que permitan a los usuarios entender el negocio de la empresa. Si bien es cierto, se maneja una gran cantidad de información, no es menos cierto que a través de las técnicas de Inteligencia de Negocios, se puede discriminar datos duplicados, datos vacíos y datos relevantes, transformando así los datos en información, después puede asegurarla para que sea confidencial, integra y disponible.

La información puede tener en su interior líneas de código que pueden dañar los sistemas de información. Estas líneas de código son generadas por personas, programadores que desean divertirse, vengarse u obtener beneficio económico de alguna persona o empresa, o por estar al servicio de la competencia o un servicio de inteligencia extranjero se inmiscuye en la red y altera su información, poniendo así a la empresa o persona en un estado de vulnerabilidad.

Salvador Carrasco asegura que: “El impacto económico de Big Data es enorme. De hecho, ya se está empleando en el marketing y la prospección comercial de forma general (planificación de campañas publicitarias, localización de centros comerciales, distribución de productos) y para el targeting y scoring individualizado en función del perfil de cada cliente, un perfil muy detallado. La información que tienen esas corporaciones sobre individuos específicos o sobre segmentos de población es lo suficientemente buena como para emplearla más allá que en inteligencia económica. Estas empresas se han convertido en grandes corporaciones en el sector de las tecnologías y la influencia que podrían ejercer por sí mismas, o empujados por los gobiernos de sus países de origen o los grupos de interés que los soportan, es enorme. Su existencia compromete el propósito original de las iniciativas como Open Data, el libre acceso a las bases de datos en manos de las administraciones públicas, o de las leyes de transparencia. Los grandes grupos del sector de la información son los que tendrán más recursos para la explotación y el cruce de esta información procedente de la Administración”. (Ramos, 2014)

2.9. Decisión Inteligente y Sistemas de Soporte para el diseño de políticas, (L. Niu, 2008)

Es un libro que contiene varios temas relacionados a los sistemas de inteligencia de negocios y el diseño de políticas en una empresa. Básicamente los dos temas relacionados a este proyecto son: Modelado del riesgo para el desarrollo de una política y Orientación Cognitiva para Sistemas de inteligencia de negocios.

Modelado de riesgos para realizar políticas, es un tema que se basa en las necesidades de las personas que realizan políticas de soporte, es decir, que requieren un conjunto de herramientas que les ayuden a la toma de decisiones en situaciones de riesgo. Estas personas necesitan un modelo donde analizan los datos que reciben de una empresa y las reglas de negocio, correlacionando esta información para generar nuevos conocimientos y poder generar nuevas políticas. Son temas muy extensos y difíciles de tratar, debido a que cada empresa gira en un negocio diferente por lo que se debe seguir una serie de técnicas para evaluar las posibilidades de generar políticas y estrategias que pueden estar orientadas a diferentes campos como seguridad de la información, económica, educacional, entre otros.

El riesgo que se corre al crear nuevas políticas, es que debido a tanta información que se usa, se puede generar información errónea por el mal manejo de los datos o el mal análisis de ellos. Por esta razón, para generar políticas se debe usar herramientas que analicen los datos que se reciba, discrimine duplicados, vacíos o simplemente datos que no tienen ninguna utilidad para el usuario final, después de obtener esos datos limpios se transformen y finalmente generen políticas de acuerdo a esa nueva información.

La manipulación de información, toma una parte muy importante, se debe “jugar” con los datos e información antigua de la empresa para correlacionar y generar nuevos resultados. Adicionalmente, cuando se crea nuevas políticas, independientemente del campo al cual están dirigidas, se debe realizar un análisis de riesgo para conocer cómo actúan las políticas y que riesgo pueden afectar dichas políticas. Las políticas tendrán una entrada, una evaluación y un impacto. Dando a conocer el impacto de cada una de las políticas en relación al negocio de una empresa. También al conocer el impacto de las políticas que se generan, se puede conocer la probabilidad de afectación de esto con relación a la empresa.

Orientación cognitiva en sistemas de inteligencia de negocios, este segundo tema está basado en los aspectos cognitivos de una persona para la toma de decisiones, se comenta que el uso de mapas mentales ayuda a que una persona resuelva problemas con facilidad y también sea más real la información que se maneja. Los sistemas de inteligencia de negocios son manejadores de información, también conocidos como los sistemas que se enfocan el manejo de grandes volúmenes de información de una empresa involucrando varios sistemas más que permiten tratar procesos para generar nuevos conocimientos y presentar alternativas para los usuarios a fin de que puedan tomar buenas decisiones para que su empresa sea más competitiva. Normalmente, un sistema de inteligencia de negocios está conformado por cuatro niveles:

- Nivel de Sistemas Operacionales: es donde se encuentra la línea de soporte del negocio, típico sistema OLTP, es decir, sistemas de procesamiento de una orden de un cliente, el sistema financiero y el sistema de recursos humanos.
- Nivel de Adquisición de Datos: este nivel tiene tres subprocesos:
 - Extracción, donde se obtiene información de los sistemas OLTP
 - Transformación, en el cual se transforma los datos que son vacíos o duplicados hasta que esta información sea limpia y unificada.
 - Carga, es el último proceso donde la información limpia es cargada en un Data Warehouse
- Nivel de Almacenamiento de Información: es en donde se encuentra la información limpia y unificada que se extrajo del nivel anterior, posee dos tablas, una llamada la tabla de hecho y la otra llamada tabla de dimensiones: Abarca toda la información de los sistemas de una empresa.
- Nivel de Análisis: finalmente, es el último nivel de un sistema de inteligencia de negocios, donde se analiza la información almacenada. Existen varios sistemas que se pueden involucrar en este nivel como: minería de datos, balanced scorecard, reportadores y sistemas OLAP. Estos permiten demostrar la información resultante en nuevo conocimiento y el usuario final conocerá el estado de su empresa y que decisiones podría tomar para mejorarla.

El objetivo principal de los sistemas de inteligencia de negocios es obtener datos y generar conocimiento para tomar decisiones apropiadas basada en esos datos

recibidos. Una vez que se tiene un sistema común de inteligencia de negocios se puede integrar con la orientación cognitiva, es decir, el uso de mapas mentales en un sistema de inteligencia de negocios. Para la fusión de estos dos conceptos: sistema de inteligencia de negocios y orientación cognitiva, se necesita de los siguientes componentes:

- Toma de decisiones naturales: es una teoría basada en el conocimiento o experiencia del ser humano, es decir, las personas son creadoras de sus propias decisiones usando sistemas de conciencia y modelos mentales.
- Sistemas de Conciencia: es crear una imagen de la empresa, donde se puede configurar sus estrategias y predicciones futuras.
- Modelos Mentales: son representaciones del ser humano para describir las cosas que suceden. Estos modelos son importantes para los supervisores de una empresa con el objeto de describir el ambiente y los problemas que la empresa tiene al momento.
- Orientación cognitiva en aplicaciones de inteligencia de negocios: es la mezcla de los tres componentes anteriores, incluyendo la psicología y el concepto de la interacción del ser humano, interviniendo conceptos como los modelos mentales de una empresa para poder predecir su futuro. Todo sistema de inteligencia de negocios puede ser investigado, diseñado, desarrollado y aplicado a la orientación cognitiva.

En esta investigación se propone un framework de un sistema de inteligencia de negocios cognitivo basado en cuatro componentes:

- Usuario: este módulo es donde la persona encargada puede gestionar los demás módulos.
- Soporte de Decisiones: módulo donde se gestiona un set o conjunto de herramientas que permita desarrollar un proceso de análisis a las decisiones que se vayan a tomar, aquí se realiza un mapa de cómo funciona cada sistema en la empresa, observando cada una de sus funcionalidades para las posibles mejoras.
- Situación de Evaluación: módulo responsable de la etapa de las decisiones y ayudas al módulo anterior. En este módulo se evalúa la información del proceso anterior para poder obtener información limpia y confiable.

- **Datawarehouse:** es el módulo donde se almacena la información limpia y confiable, sin datos duplicados, ni vacíos, son datos que se presentarán a las personas para que puedan tomar decisiones y predecir sus negocios.

En conclusión, los sistemas de inteligencia de negocios pueden ser integrados con otros sistemas relacionados con la percepción humana, para la mejora de toma de decisiones y ahorro de recursos. Sin embargo, es un proceso mediante el cual se debe conocer el negocio de la empresa para poder realizar el mapeo de la misma. Así se conocerá el giro de negocio y sus funciones, pudiendo desarrollar un sistema de decisiones mejorado y que presente información veraz y factible para los usuarios finales.

2.10. Estrategias Nacionales de Ciberseguridad (E. Leiva, 2015)

Esta investigación determina que existen muchas herramientas para realizar ataques por la inseguridad que hay en el ciber espacio, por esta razón, proponen estrategias de ciberseguridad, para la protección de la información de una empresa. Las políticas de ciberseguridad pueden ser muy necesarias no solamente a nivel empresarial sino a nivel nacional, es por esto que se realiza un análisis comparativo entre varios países que poseen políticas de ciberseguridad, sus ventajas y desventajas.

La ciberseguridad es un conjunto de herramientas y políticas que permiten controlar el acceso a las redes de los sistemas y proteger la información que se maneje en ella. La propuesta de realizar estrategias de ciberseguridad se puede tomar como un elemento que ayude la protección de lo más valioso de una empresa, sus datos, pero sobre todo ayudar a prevenir cualquier acceso indebido. Los países en vías de desarrollo no poseen políticas ni estrategias de ciberseguridad, sin embargo, hay algunos que se las han considerado debido al uso de nuevas tecnologías.

Ciberdefensa: es la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques. (J. LoroseMe, 2015)

Ciberseguridad: se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Teniendo en cuenta los conceptos básicos, proceden a establecer una estrategia o política de ciberseguridad que proteja: Infraestructura, Economía, Seguridad Nacional y el Bienestar Social, es decir, estas políticas o estrategias deben estar enfocadas hacia: concientización, conocimiento, ciberseguridad y capacidad cibernética militar. Las políticas de ciberseguridad, deberían estar basadas en estrategias o políticas creadas anteriormente, en esta investigación se habla de colaboraciones entre naciones que se encuentran no solo desarrollando estrategias sino también países que ya las tienen establecidas. Para poderlas crear se debe realizar un análisis de las amenazas que el ciberespacio posee y manejar varios conceptos de seguridad que permitan proteger no solo la información sino también la infraestructura de una empresa.

Una complicación para realizar políticas en los países en desarrollo es la falta de recursos para detectar amenazas en el ciberespacio y la falta de personal especializado en las áreas de seguridad. Por estas dos razones, los países en desarrollo no poseen ni estrategias ni políticas de ciberseguridad y hace que sean vulnerables; por otra parte, los países de Europa, han desarrollado algunas estrategias para proteger su información. El análisis de las amenazas a que una empresa o el estado podrían estar propenso, se realiza a través de un proceso de pruebas, es decir, ejecutar varias herramientas de hackeo, barridos de red, escaneos de puertos, entre otras, especialmente en sistemas financieros para luego desarrollar medidas de seguridad. Existen también herramientas de libre acceso, pero los conocimientos son los que pueden fallar, personas que no están preparadas en temas de seguridad de la información o sobre el ciberespacio, podría también perjudicar a la creación de políticas.

En los últimos años, se ha tratado de integrar a todos los países para el desarrollo de estas estrategias o de políticas de seguridad. Esto se debe a que la información de una empresa o de un estado no se puede encontrar circulando por la Internet sin las debidas medidas de seguridad y afectar a todos.

2.11. Políticas Nacionales de Ciberseguridad

Debido a los avances tecnológicos que en los últimos años se ha obtenido, el Internet, se ha convertido en una herramienta importante para la comunicación entre empresas y por ende entre países. Sin embargo, esta comunicación ha sido en ciertas

partes beneficiosa, porque mantiene comunicados y compartiendo información entre ellas. Por otro lado, también ha sido de gran desventaja porque hace que la información sea vulnerable a amenazas y robo de la misma. Para ello se ha creado una “Declaración de Principios de la Sociedad de la Información”.

La Declaración de Principios de la Sociedad de la Información (2003, WSIS-03/GENEVA/4-S) es un documento escrito por la Unión Internacional de Telecomunicaciones (UIT) basada en los comentarios y conclusiones obtenidas después de la realización de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI).

Los participantes, a través de este documento declaran el deseo y compromiso común de: “construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos”.

Según el Informe de la Declaración de Principios, para lograr una adecuada gestión de Internet se deben abarcar cuestiones técnicas y de política pública, y contar con la participación democrática de todos los interesados, a fin de garantizar “la distribución equitativa de recursos, y un funcionamiento estable y seguro de Internet”. Además de la inclusión de organizaciones internacionales e intergubernamentales competentes como veedores de dicha gestión. Por este motivo, en el informe se reconoce que:

- “la autoridad de política en materia de política pública relacionada con Internet es un derecho soberano de los Estados. Ellos tienen derechos y responsabilidades en las cuestiones de política pública internacional relacionadas con Internet;
- el sector privado ha desempeñado, y debe seguir desempeñando, un importante papel en el desarrollo de Internet, en los campos técnico y económico;
- la sociedad civil también ha desempeñado, y debe seguir desempeñando, un importante papel en asuntos relacionados con Internet, especialmente a nivel comunitario;

- las organizaciones intergubernamentales han desempeñado, y deben seguir desempeñando, un papel de facilitador en la coordinación de las cuestiones de política pública relacionadas con Internet;
- las organizaciones internacionales han desempeñado, y deben seguir desempeñando, una importante función en la elaboración de normas técnicas y políticas pertinentes relativas a Internet”.

Este informe permite a las naciones manejar políticas internas para proteger la información interna y externa de cada empresa, logrando que cada país tenga una ley donde se proteja no solo la información de las personas sino también la información de las empresas dentro y fuera del mismo.

El Ecuador, al ser un país en desarrollo posee ciertas limitaciones en cuanto a conocimientos, recursos humanos y financieros para participar en una cumbre como la anteriormente mencionada. Sin embargo, en las reuniones posteriores, Ecuador, fue nombrado, impulsando así el estudio de nuevas políticas o adaptaciones de las mismas de acuerdo a cada uno de los países con el debido estudio de su entorno.

El 16 de marzo de 2010, se presentó ante la Asamblea Nacional el proyecto de “Ley de Protección a la Intimidación y a los Datos personales”, donde se habla de la protección de los datos de las personas y la información de cada una de las empresas. Un ejemplo de esta propuesta es: “Se prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas”.

En los últimos años, la información en las empresas ha crecido enormemente, muchas de las veces perdiendo un control en su seguridad. La información es lo más importante que una empresa puede tener, se debe cuidar sin importar el “gasto” que esta puede implicar. A pesar de estas nuevas tendencias no existen muchos estudios referentes políticas de ciberseguridad. Sin embargo, se encontró un estudio enfocado a las políticas de conectividad o relacionadas con las TICs, recordando que cada

empresa puede tener sus propias políticas de seguridad de la información manejadas con las políticas del gobierno (Políticas de conectividad a las TIC desde un enfoque de derechos. Especial atención al caso de Ecuador Políticas de conectividad a las TIC desde un enfoque de derechos)

2.12. Acerca de la soberanía del Ecuador en el ciberespacio.

Es una investigación sobre la soberanía del Ecuador en el ciberespacio, que se refiere a una cultura del “todo conectado”, donde se explica claramente que al haber información en la nube o que se encuentra conectada con ella, muchas personas pueden tener acceso y puede ser usada en diferentes formas, sea para fines de estudio o simplemente para hacer daño a cualquier empresa. Adicionalmente, se habla de políticas a nivel continente, a nivel país y a nivel regional, donde se enfoca básicamente en las políticas o estándares que se debe seguir para que las conexiones de las TIC tengan seguridad y la información sea confiable e íntegra. Habla también de Big Data, y los grandes volúmenes de información que hoy en día maneja y los descuidos que se puede tener en puertos o simplemente en las conexiones de dispositivos. Es muy complicado establecer una seguridad de información al 100%, sin embargo, no es imposible si se empieza por generar objetivos claros con estrategias precisas.

Los ataques a la información han evolucionado, ahora no solo es definir un sistema operativo o una solución de seguridad para que los sistemas de las empresas se encuentren seguros, porque todos tienen sus vulnerabilidades y pueden estar sujetos a cualquier tipo de ataque. Es más bien una cuestión de analizar la lógica del negocio y establecer las estrategias de seguridad necesarias para que la información se encuentre protegida, viable y garantizar no solo la soberanía de la información sino la soberanía de las personas.

Tanto la ciberseguridad como el concepto de Big Data, son términos que llaman mucho la atención debido a la extracción de grandes cantidades de información que pueden ser útiles para generación de políticas o de estrategias de seguridad y pueden permitir la toma de decisiones en las empresas, asegurando su información y su mejorando su competitividad. El tratamiento de grandes volúmenes de información permite la correlación de conceptos que permiten generar nuevo conocimiento. (Ramos, 2014).

En Ecuador, no existen políticas nacionales de seguridad que protejan la información que se maneja dentro y fuera del país y es por esta razón se propone este tema relacionando dos conceptos: la ciberseguridad y la inteligencia de negocios, para conocer las políticas que se puede generar en Ecuador y poder ser replicadas en cada empresa, no solo en las públicas sino en las privadas y cuidar la información del país en general.

2.13. Métodos de Investigación de Campo.

La investigación de campo es un proceso que, utilizando el método científico, permite obtener conocimiento en el campo que se desarrolla un fenómeno. Las técnicas que se usa en esta investigación de Campos son (Krause, 1995):

- Observación: consiste en técnicas formales e informales que permiten la recolección de datos que puedan ayudar a la investigación del tema propuesto.
- Cuestionarios: son herramientas que permiten realizar varias preguntas referentes al tema de investigación a personas que se encuentran involucradas en el tema.
- Entrevistas: instrumentos que permiten a la recolección de la información relevante para ayudar a la investigación en forma directa y personal.

En esta investigación se utilizará cuestionarios y entrevistas a varias empresas, mediante las cuales se conocerá las políticas de la seguridad de la información, que se maneja a nivel de empresas públicas y privadas.

2.14. El método Delphi.

Es una técnica para obtener información cualitativa mediante la elección de un grupo de expertos que expresen su opinión acerca del tema de investigación y sus propuestas de futuro orientadas a ese tema. Básicamente, está orientada a realizar cuestionarios, formulando preguntas referentes al tema de investigación teniendo respuestas que ayuden a tener un conocimiento del problema y su solución. Para ello, el método Delphi tiene cuatro fases (Astigarraga, 2006):

- Fase 1: Formulación del Problema: es una de las fases más importantes en este método, aquí se define el campo donde se realizará las preguntas de las herramientas de recolección de datos. Es la parte fundamental y de donde los investigadores empiezan a realizar su investigación.
- Fase 2: Elección de los Expertos (L. JIMENEZ): esta fase se caracteriza por la elección de un grupo de expertos en el tema del problema principal de la

investigación. Básicamente se colecta opiniones a través de los correos electrónicos debido a que esta técnica se basa en la opinión anónima acerca del tema de investigación.

- Fase 3: Elaboración y Lanzamiento de los cuestionarios: esta fase, se relaciona con la fase anterior, de acuerdo al grupo de expertos seleccionados, se realiza las preguntas necesarias que permita ejecutar una investigación precisa del tema propuesto.
- Fase 4: Desarrollo práctico y explotación de resultados: esta última fase, se refiere a la ejecución de los cuestionarios y de acuerdo a la recepción de la información se puede obtener los resultados a la investigación propuesta.



Figura 5 Fases del Método Delphi

El método Delphi se aplica para la investigación de patrones de ciberseguridad, usando herramientas de Inteligencia de Negocios. Esto se debe a la necesidad de prevención de nuevas vulnerabilidades y amenazas que existen en estos últimos años.

CAPÍTULO 3.- METODOLOGÍA DE LA INVESTIGACIÓN

En este capítulo se desarrolla el trabajo de campo de la investigación, realizado a través de un procedimiento sistemático de división del objetivo general en objetivos específicos sucesivos, que al cumplirse sirven de base para el siguiente, esto no restringe la posibilidad de regresar a algún objetivo si es necesario reacondicionarlo. Cada objetivo se consigue con una secuencia de actividades, como se detalla a continuación.

3.1-Objetivo Específico N° 1.

Es importante establecer en forma clara la relación existente e importante de los patrones que se utilizan en este tipo de tecnología; por tanto, el objetivo Nro. 1 es: Analizar el uso, aplicabilidad y proyección de patrones en ciberseguridad y su relación con BI.

Ubicación Geográfica y alcance

La investigación se encuentra referida al ámbito nacional e internacional, por tanto, se realizará considerando la influencia de la tecnología y procedimientos adoptados internacionalmente, mediante una investigación bibliográfica o documental se cumple este con ayuda de consultas a organismos y empresas relacionadas.

Identificación de variables/ categorías a utilizar en el proceso investigativo.

Se identifican las variables derivadas del objetivo y se describe a continuación su ámbito de búsqueda y análisis.

- Patrones: se refiere a los diferentes tipos de conceptos de patrones como: patrones en forma general, patrones de Inteligencia de Negocios, patrones de ciberseguridad.
- Patrones en Inteligencia de Negocios: es una variable referente a patrones de tiempo, patrones de conducta, patrones de secuencia.
- Patrones en Ciberseguridad: se refiere a conceptos de actividades repetitivas en el ámbito de la ciberseguridad.
- Uso de patrones: comprende el uso de patrones, tanto en forma general como específica en BI (Inteligencia de Negocios) y en Ciberseguridad, ejemplos de

proyectos realizados o herramientas utilizados, estado del arte en el empleo de patrones en ciberseguridad en el mundo y en el Ecuador.

- Aplicabilidad: esta variable se refiere a la utilidad, facilidad de aplicación, conveniencia, costos e infraestructura necesaria de los patrones.
- Proyección: Cómo podrían ser utilizadas en el futuro y cuál es la tendencia.

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

Se describe a continuación los métodos, herramientas e instrumentos que se utilizan para la investigación y resolución de cada una de las variables planteadas.

- Investigación documental: se emplea un plan de investigación de campo en el que se describe las variables relacionadas con las fuentes disponibles, al momento en la IEEE, Scopus y Bibliotecas de la ESPE Digital.
- Investigación de campo: Se elaboran varios instrumentos como: Encuestas y entrevistas a empresas y organismos relacionados; recopilando la información en instrumentos como: histogramas y gráficas de pastel para su evaluación.

Desarrollo de la Investigación

Se realiza una revisión sistemática en varios artículos científicos y libros relacionados, en los que se establece la condición de cada uno de las variables antes indicadas.

- **Patrones.**

Es una acepción general para describir un procedimiento de comparación de una actividad repetitiva particular en una situación específica que se lleva a cabo dentro de un marco definido, que puede ser utilizada con frecuencia en un modelo establecido (Yorio, 2006). Con el uso de herramientas de BI, como señala Baumgartner en su artículo técnico (Baumgartner, 2005), los patrones son “un conocimiento creado por la extracción, análisis y estructuración de información que puede ser usada de forma repetitiva en futuros trabajos relacionados a ese dominio”, menciona que los patrones, son formados por varias condiciones de acuerdo al dominio de la información.

Para la Inteligencia de Negocios, un patrón también puede ser considerado como: “la extracción de información relevante usando herramientas de minería de datos” (Golfarelli, 2004).

Sin embargo, en ciberseguridad el concepto de patrones cobra gran importancia, porque se conforman sistemas de defensa contra fraudes o lavado de dinero en los que se considera como el comportamiento inusual de un usuario en una cuenta que ha sido monitoreada.

- **Uso de patrones**

La seguridad en el intercambio de información entre las organizaciones y unidades de negocio, es un problema común y de gran importancia en los últimos años. El análisis de grandes volúmenes de datos o analítica de Big Data, puede ayudar a resolver la seguridad de la información que muchas empresas usan y proporcionar la inteligencia de datos que detecta patrones sospechosos y amenazas potenciales, mediante la ampliación de la definición de seguridad de los datos a todas las partes del negocio. (Richards, s.f.).

La seguridad de la información guiada por la inteligencia de negocios e impulsada por la analítica de Big Data será una disrupción en varios productos de seguridad informática en los próximos años, debido a que tanto las personas como las empresas, nunca imaginaron que la información que se maneja hoy en día ocuparía grandes volúmenes de información y en muchos casos, se transformaría en información que no sea usada y que sea más vulnerable que antes.

Actualmente las organizaciones y empleados operan cada vez más en ambientes móviles, de redes sociales y Web; aprovechando la información identificada por análisis o patrones en una amplia variedad de conjuntos de datos, incluyendo texto no estructurado y datos binarios –audio, imágenes y video– se puede ofrecer información valiosa sobre los riesgos de la empresa. Existen algunas amenazas que no pueden ser identificadas a pesar del uso de modelos estadísticos o el análisis predictivo que ha sido desarrollado, sin embargo, la pregunta que las personas se hacen es: ¿Los grandes volúmenes de datos y el análisis de alto rendimiento mejorará la seguridad de la información? Se podría decir que sí, pero hoy en día el uso significativo de las tecnologías de Big data en grandes volúmenes de datos para seguridad es completamente extraño y

representa muchos retos especialmente económicos, por lo que muchas empresas no estarían dispuestas a invertir en herramientas ni en la creación de estrategias ni políticas de seguridad.

Existen actualmente muchas empresas que usan tecnología de seguridad de la información y gestión de eventos (SIEM) para analizar los log que almacenan eventos de la red y que incluye los datos de todos los sistemas, "Internet de las cosas" y dispositivos conectados, incluyendo cualquier texto ASCII que pueda ser indexado, puede utilizar hasta 150 comandos en los datos de retorno establecidos para llevar a cabo el análisis estadístico y hacer visualizaciones.

Existen empresas que prestan servicios de analítica de Big data, Opera Solutions por ejemplo, especializada en análisis predictivo, utiliza el aprendizaje de las máquinas para reconocer patrones en los datos de código abierto como páginas vistas o la información de Twitter y para abstraer inteligencia predictiva a partir de los flujos de Big Data. Esta empresa utiliza ontología de amenazas de 80 millones de palabras y extrae frases multilingües en 15 idiomas, se da prioridad a las frases por niveles de amenaza, sobre la base de unos 450 millones de relaciones entre esas palabras, generando así patrones que identifican la variedad de las amenazas en tiempo real y de esa manera se pueda prevenir nuevos ataques.

Los servicios de análisis de grandes volúmenes de datos están orientados a los sectores gubernamentales y comerciales, sin embargo, se debería orientar a todo tipo de empresa y personas, porque todos están expuestos a amenazas del ciberespacio.

Existe una herramienta desarrollada por los estudiantes de la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid (UPM), que se basa en el estudio de minería de datos y recibe información que puede ser estudiada, analizada y extraída para fines de ciberseguridad y prevención de fraudes informáticos. Esta herramienta permite realizar un proceso en el cual se recolecta información, se analiza a través de ontologías, usa inteligencia artificial y por último genera nuevo conocimiento, permite así

reconocer los fraudes de los últimos años y ayuda a las personas a tener un conocimiento real de la ciberseguridad. (Universidad Politécnica de Madrid, s.f.).

También, se puede rescatar un estudio realizado por estudiantes de la Universidad Latinoamericana de Ciencia y Tecnología, ULACIT, de la ciudad de Costa Rica. Estas personas usan una herramienta llamada Snort Traffic, es un sistema de análisis de paquetes, que detecta y registra intrusiones y ataques de red en tiempo real, permitiendo a los estudiantes recolectar información sobre los patrones de ataque de ciberseguridad, estos patrones, básicamente se refieren a información anteriormente analizada y estudiada que se presenta en tiempo real. El nuevo conocimiento que genera, se basa en patrones de conducta estudiados anteriormente, con información recolectada en tiempos pasados, usa lógica difusa y realiza predicciones futuras.

Los patrones de ciberseguridad no sólo se pueden usar para defensa de una empresa, sino que también se puede usar para atacarlas. Los antivirus salieron al mercado por la creación de virus, sus patrones podrían actuar de la misma forma: ser creados para prevenir un ataque o una amenaza y también generar patrones para atacar a una empresa de acuerdo al tipo de información que maneje.

Existen varios prototipos de sistemas que permiten la prevención de intrusos a través del uso de patrones de ataques de la información (Y.A.A., 2010), estos patrones son diseñados de acuerdo a los ataques suscitados en los últimos años a diversas organizaciones. Esta nueva estrategia de crear patrones de acuerdo a sucesos anteriores va a permitir aplicar de forma eficaz medidas de contención y eliminación de ataques.

Los patrones de conducta de una empresa pueden ser usados para realizar nuevos ataques a las empresas, debido a la información que se puede obtener con ellos. Las empresas no solamente deben estar pendientes de la protección de la información sino del uso de la misma, porque que los usuarios pueden dar a conocer mucha información a través de patrones de comportamiento o de conducta.

La aplicabilidad de los patrones de seguridad se puede visualizar en diferentes aspectos como la creación de contraseñas, es decir, seguir un modelo en el cual

se base para crear nuevas cosas, la creación de nuevos conocimientos que ayuden a las empresas a la creación de estrategias de ciberseguridad o políticas de ciberseguridad y permitan la prevención de amenazas y controlar las vulnerabilidades de la información. La aplicación de estos patrones, requieren su tiempo de maduración dependiendo de las herramientas que se vayan a usar, por ejemplo, la empresa HP lanzó una herramienta llamada HP SureStart, para la prevención de fraudes y protección de las empresas, herramienta orientada a la ciberseguridad de la empresa, evitando virus y bots, asegurándose que la empresa no tenga ningún problema y si el acceso a la web es imposible sería a causa de algún patrón de seguridad que fue encontrado.

Según la revista “Gestión de la información”, existen varios tipos de patrones: Patrones de ataque, Patrones de comportamiento y Patrones de conducta, usados en herramientas de Big Data para la prevención de fraudes, ataques y detección de nuevas vulnerabilidades de la información. También pueden ser usados para comprobar la vulnerabilidad de la información, conociendo estos patrones se puede realizar un análisis mediante el cual puede hacer que la información sea más vulnerable.

La creación de patrones de ciberseguridad es complejo debido a la infraestructura que maneja cada empresa, existen muchas herramientas que pueden proporcionar nuevos conocimientos y crear patrones de acuerdo a los dominios que se maneje. En el blog de ciberseguridad de Vión (Vión, s.f.), se considera como un cambio complejo y de grandes retos, debido a la información que se maneja hoy en día, se debe conocer el “quién”, “cómo”, “dónde”, “cuándo” y “porqué” de la información, para establecer nuevos conocimientos y usarlos en la prevención de las amenazas a la seguridad de la información. La información debe ser tratada y analizada de la mejor manera para realizar predicciones acertadas y construir estrategias o políticas de ciberseguridad para una empresa y a nivel nacional.

La proyección a futuro de los patrones de ciberseguridad se orienta a los cambios de tecnología que manejan las empresas, que ahora ya no manejan

información con su propia infraestructura física sino que lo hacen en la nube, con el consecuente riesgo.

Según el INCIBE (INCIBE, s.f.), las tendencias de la ciberseguridad y por ende la creación de patrones se basa en siete sectores:

- Sector Industrial y Medio Ambiente, que se refiere a la protección y seguridad de los dispositivos y redes de la infraestructura que se maneja en este sector.
- Sector Movilidad, los objetivos de ciberseguridad se fundamentan en la protección de medios de transporte aéreo o terrestre, o dispositivos móviles que requieran de comunicación satelital.
- Sector Servicios, en el que se incluye la división financiera y de seguros, cuya finalidad en ciberseguridad se asienta principalmente en la defensa y protección contra incidentes derivados de la digitalización de sus servicios, tales como la banca online o los servicios y aplicaciones Fintech.
- Sector Ciudadanía, que incluye los servicios públicos básicos de sanidad y educación, cuenta con necesidades en ciberseguridad, por un lado, orientadas hacia la protección de dispositivos médicos interconectados, patentes o información sensible de pacientes utilizadas en el ámbito sanitario y farmacéutico.
- Sector Gobernanza, basado en los organismos públicos y Administraciones Públicas y sus correspondientes vulnerabilidades en ciberseguridad derivadas del control y gestión de información y servicios públicos ciudadanos electrónicos, fundamentalmente.
- Sector TIC, basado en la digitalización, es un sector transversal a los anteriores que recopila las necesidades y prácticas más habituales en materia de ciberseguridad, ofrecidas desde un entorno como la nube, y las cuales pueden ser aplicadas al resto de sectores definidos.

Los expertos de SophosLabs (SophosLabs, s.f.), han determinado las tendencias más relevantes para el año 2016, basados en la recolección de datos y análisis de los mayores avances tecnológicos, que serían las siguientes:

- Las amenazas a dispositivos móviles (Android e iOS).- Cada año los dispositivos móviles están tomando más y más la vida de las personas y estas

no podrían sobrevivir sin ellos, por esta razón los dispositivos móviles son herramientas que serán más vulnerables en el ciberespacio para cualquier ataque. Los patrones de ciberseguridad podrían estar orientados a estos dispositivos para prevenir cualquier amenaza y conocer la información que se expone a nuevas amenazas y vulnerabilidades.

- Internet de las cosas (IoT).- Son dispositivos que conectan todo lo que nos rodea, y constantemente están apareciendo nuevos casos de uso. El IoT seguirá siendo un foco de noticias basadas en el hecho de que los dispositivos son inseguros, por esta razón se debe prevenir cualquier ataque o amenaza en estos dispositivos. Los patrones de ciberseguridad pueden tomar un papel muy importante, porque permitirán prevenir cualquier amenaza, determinar las vulnerabilidades de la información de estos dispositivos y crear conocimiento que puede ayudar a mitigar su impacto.
- Las pymes se convertirán en mayor objetivo para los ciberdelincuentes, porque son consideradas como blancos fáciles, por lo que estas empresas deben enfocarse en la seguridad de su información. En este caso los patrones de ciberseguridad sería una muy buena oportunidad para evitar ataques y asegurar la información.
- Ingeniería social.- Las empresas y las personas deben protegerse de este fenómeno debido a que cada año se ha detectado más ataques causados a través de este tipo de actividad humana. Los patrones de ciberseguridad podrían analizar los anteriores ataques y empezar a generar nuevos conocimientos para prevenirlos.

3.2-Objetivo Específico N° 2.

Analizar las políticas nacionales referidas al campo de la Ciberseguridad que el Ecuador posee actualmente y si estas tienen alguna relación con la Inteligencia de Negocios.

Ubicación geográfica y alcance.

El análisis de las políticas nacionales orientadas a la Ciberseguridad, estará basado en las regulaciones que la República del Ecuador tiene para regular acciones jurídicas

orientadas al uso de las tecnologías. La investigación se realiza a nivel nacional, comprobando la existencia de políticas de ciberseguridad, y si estas son usadas en el ámbito de la Inteligencia de Negocios.

Identificación de variables/ categorías a utilizar en el proceso investigativo.

Las variables identificadas son las siguientes:

- Políticas nacionales de ciberseguridad en Ecuador.
- Estudios o normativas relacionadas.
- Legislación Internacional.
- Legislación de Ecuador referente a Internet.
- La interceptación ilegal de datos.
- Leyes sobre Seguridad Informática.

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

Los métodos, herramientas e instrumentos que se utilizan para la investigación, son básicamente los siguientes:

- Investigación documental
- Investigación de campo.

Desarrollo de la Investigación

- **Políticas nacionales de ciberseguridad en Ecuador:**

En la República del Ecuador, no existen políticas generales para las empresas ni para las personas que usan la Internet, sin embargo, en los últimos años existe la tendencia de invitar a los países en desarrollo a las conferencias de ciberseguridad de nivel mundial, para propiciar la seguridad de la información que manejan las personas y las entidades tanto públicas como privadas en sus naciones.

Existen disposiciones constitucionales y legales, así como reglamentarias y acuerdos ministeriales referidos a la seguridad de la información, leyes específicas de protección de datos y privacidad que se encuentran en trámite de aprobación en la Asamblea Nacional, pero no se ha configurado una Política

Nacional de Ciberseguridad como en otros países de la región; es el ejemplo de Colombia que ha avanzado significativamente en ese aspecto, Perú y Brasil.

Las empresas y organizaciones públicas y privadas han tomado sus propias iniciativas tratando de asegurar la información de sus negocios y sus clientes, para no perder competitividad en el mercado.

- **Estudios o normativas relacionadas:**

Debido a la existencia de actividades criminales a nivel informático se han creado leyes y regulaciones para proteger los derechos constitucionales de las personas naturales y jurídicas que usan las TIC, dando también normas para esas actividades. Para que la regulación sea efectiva, es necesario conocer primero los tipos de delitos informáticos que existen hoy en día. La Organización de Naciones Unidas (ONU) reconoce oficialmente los siguientes tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de computadoras
- Manipulación de los datos de entrada
- Daños o modificaciones de programas o datos computarizados

Al conocer los tipos de delitos informáticos, también se puede saber las personas que intervienen en los mismos como: sujeto activo (delincuente) y sujeto pasivo (víctima).

- **Legislación Internacional:**

En los últimos años, se ha desarrollado en el ámbito internacional, un estudio en los diferentes ámbitos tanto político como jurídico de los problemas derivados del mal uso de las computadoras y de la Internet, que ha dado lugar en algunos casos, a la modificación del Derechos Penal nacional e internacional. La ONU señala que los delitos informáticos forman parte de un crimen transnacional, que involucra a todos los países del mundo y que por esta razón, habrá que recurrir a los tratados internacionales para actuar en forma eficaz contra esta amenaza que aqueja al planeta en su totalidad y que causa serios problemas económicos, geopolíticos y sociales.

Existen países que han desarrollado legislación orientada al uso de la información y a su seguridad como: Alemania, Austria, Chile, China, España, Estados Unidos, Francia, Holanda e Inglaterra.

Sin embargo, no todos los países cuentan con una legislación apropiada que regule actividades criminales o el uso indebido de la tecnología. Como se puede observar en Ecuador, no se cuenta con una legislación para regularizar el uso de los datos ni proteger la información que se comparte por la red.

La legislación no solo se debe pensar en cómo una forma de castigo, sino algo mucho más importante cómo probar el delito y prevenir nuevos delitos informáticos. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día.

- **Legislación de Ecuador referente a la Internet.**

En Ecuador, se han presentado una serie de acontecimientos ilícitos con la información y los datos que manejan una entidad o empresa. La Fiscalía General del Estado, ha recibido denuncias relacionadas con transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, pornografía infantil, acoso sexual, entre otros delitos similares.

La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal (COIP)- hasta el 31 de mayo del 2015. En el COIP se sancionan los delitos informáticos, cuyos actos se cometen con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales, sin embargo, especialistas en delitos informáticos, afirman que en Ecuador existen dificultades durante la investigación de delitos propiciados por el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país, esto se debe que todos los servidores o bancos de datos de los proveedores de estos servicios se encuentran fuera del país y es complicado acceder a esa información.

Un inconveniente para la investigación es la falta de convenios internacionales que faciliten el cruce de datos informáticos -como los que existe entre Estados Unidos y Europa-, por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la

sustracción de información personal. Las formalidades y la virtualidad de los trámites pueden tardar meses. Existen sentencias por algunos crímenes informáticos, pero estos no son tomados muy en cuenta por las diferentes políticas o leyes que se maneja en el país.

- **La interceptación ilegal de datos:**

La interceptación ilegal de datos es uno de los delitos informáticos menos denunciados de acuerdo a la Fiscalía, a pesar de que es uno de los más comunes y fáciles de ejecutar porque no se necesita de conocimientos avanzados de informática. El delito de interceptación ilegal de datos consta en el artículo 230 del COIP y se sanciona con tres a cinco años de pena privativa de libertad a quienes utilicen los datos en forma no autorizada.

Otro delito muy común es el que se comete por medios electrónicos, es el uso de adolescentes con fines sexuales o pornográficos, donde se propicia la inducción, promoción y facilitan la prostitución de un menor de edad. A estos actos, el COIP sanciona en el artículo 174, con una pena privativa de libertad de siete a 10 años. (Fiscalía, s.f.)

- **Leyes sobre Seguridad Informática**

Con el avance de la tecnología se ha generado una evolución en el ámbito empresarial y financiero de cada uno de los países así como el incremento del uso de las computadoras, comercio electrónico, contratos informáticos e intercambio de datos entre personas naturales y jurídicas.

Así como el Comercio Electrónico ofrece ventajas, también surgen nuevos problemas como son:

- La validez legal de los contratos electrónicos.
- El control de las transacciones internacionales
- La protección de los derechos de propiedad
- La seguridad y confiabilidad en el intercambio de datos electrónicos

El uso de la red es una gran ventaja que las entidades bancarias aprovechan para brindar comodidad a sus clientes y mejorar su calidad de servicio, sin embargo, esto hace que el riesgo sea también más grande en por las vulnerabilidades de los sistemas que afectan a las transferencias electrónicas de

dinero, especialmente en el uso de claves; esto se debe a la falta de medidas de seguridad y respaldo legal para prevenir y sancionar los hechos delictivos.

La legislación penal contempla aspectos relativos a la manipulación informática, uso indebido de datos informáticos, así como acceso y uso ilegal de datos; sin embargo no contempla temas como sabotaje, espionaje informático y otras figuras de fraude informático que últimamente afectan a las empresas y las entidades bancarias. Por esta razón, es necesario implementar medidas de seguridad, tanto técnicas como jurídicas, para prevenir y sancionar los fraudes informáticos, buscando también concordancia o compatibilidad con las leyes del contexto internacional, en particular de la región. (Leyes de Seguridad Informática, s.f.)

El Ecuador no establece definiciones de carácter importante que ayuden a una regularización del uso del Internet, así como Hacker, Cracker, Delitos informáticos, entre otros, al igual, se puede determinar que existe leyes que pueden prevenir delitos informáticos, sin embargo, el problema de determinar un delito informático recae en la información manipulada por el empleado, es decir, si éste usa la información de la empresa para otros fines, o tal vez que en lugar de usar la Internet para su trabajo, sea usado para realizar actividades personales, se puede ver entonces que hace falta políticas de cada empresa para regularizar el uso de la Internet, sin embargo, el establecimiento de políticas de seguridad requiere de una entidad pública o gubernamental que las audite. (Leyes y Regulaciones, s.f.)

De acuerdo al estudio realizado por Daniela Cepeda (Lavado de Dinero, s.f.), toda casa de valor o entidad financiera tiene un convenio que permite compartir las bases de datos entre ellas, siempre y cuando se cumpla ciertas condiciones, pero además, deberán regirse y cumplir con normas de seguridad de la información para que puedan seguir funcionando en el país. El riesgo en seguridad informática para una empresa está enfocado en tres componentes: datos, recursos o equipamiento y reputación o imagen que tienen enfrente a sus clientes y proveedores. Para establecer cualquier política de seguridad, en este estudio establece dos posturas: La de negociación preestablecida, en que se especifica sólo lo que se permite y se prohíbe todo lo demás. Es decir: lo que no

está permitido expresamente, está prohibido, constituyendo por lo tanto una postura de falla segura. Los diferentes servicios se van activando según el caso y la postura de permiso preestablecido, en donde se especifica sólo lo que se prohíbe y se permite todo lo demás.

De acuerdo a Delloite, en las empresas que cuentan con procesos integrados, la seguridad de la información está compartida entre el riesgo, la probabilidad y el impacto en sus procesos. Las empresas pueden integrar varias áreas y compartir información entre ellas, pero al tener una red compartida, se pueden presentar accesos indebidos y otras amenazas a la información en cada departamento, cualesquiera de estas amenazas afectan la productividad de una empresa, es necesario conocer el impacto de las mismas determinar si el riesgo es de bajo, medio o alto impacto. En relación a esto, la empresa Delloite, así como muchas otras ha presentado un portafolio de herramientas o soluciones que se enfoquen en: Mantener, evaluar, implementar y diseñar un marco de seguridad, abarcando no sólo la infraestructura sino también software. Estas las soluciones no usan Inteligencia de Negocios, pero pueden estar abiertas para el empleo con ella para cubrir los siguientes aspectos (Deloitte, s.f.).

3.3-Objetivo Específico Nº 3.

Determinar el impacto de las políticas nacionales implementadas en el país.

Ubicación Geográfica y alcance.

La investigación de campo se realiza a nivel nacional, de acuerdo a las políticas implementadas en la República de Ecuador, para conocer el impacto que ocasiona cada una de ellas, pero la investigación documental es a nivel mundial.

Identificación de variables/ categorías a utilizar en el proceso investigativo.

Las variables identificadas son las siguientes:

- Ciberseguridad con BI
- Impacto de las políticas.

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

Los métodos, herramientas e instrumentos que se utilizan para la investigación, son básicamente los siguientes:

- Investigación documental
- Investigación de campo.

Desarrollo de la Investigación

- **Ciberseguridad con BI.**

La ciberseguridad en la actualidad, es una de las orientaciones más importantes de la informática, sin embargo, la tendencia al manejo de grandes volúmenes de información va de la mano, por lo que los profesionales encargados de la seguridad de la información tienen que conocer aspectos relacionados con estas dos disciplinas: la ciberseguridad y la inteligencia de negocios, porque de esta manera ofrecen a los usuarios una gama más amplia de tecnologías y métodos que sirven para proteger la información y defenderse de los ataques que cada día son más difíciles de controlar.

La Inteligencia de Negocios, es conocida para la toma de decisiones en una empresa, pero hoy en día, la fusión de la ciberseguridad con la inteligencia de negocios puede ser fundamental para la prevención de varias amenazas que pueden afectar una empresa, especialmente con el uso de patrones y otras herramientas inteligentes, que hacen que la labor analítica se realice con la velocidad requerida y la eficacia necesaria en caso de ataques a la seguridad de la información.

- **Impacto de las políticas.**

Las estrategias y políticas en una empresa regidas por una entidad gubernamental, crea un impacto alto debido a la protección de datos que cada empresa maneja ya sea en la parte interna o externa.

A través de un análisis de los riesgos de la ciberseguridad se podrá conocer el impacto que una política puede generar no solo a nivel empresarial sino estatal.

El 7 de junio de 2016, se publicó un reportaje en Europa, en el que se determina el impacto de las políticas de ciberseguridad y la prevención de datos en ese continente. El reportaje señala que el problema no es la seguridad en sí misma

sino la protección de los activos, que es algo en lo que no se enfocan las empresas actualmente y por tanto los proveedores, clientes y consumidores deben estar de acuerdo en trabajar en forma colaborativa para prevenir nuevos ataques, contando por supuesto con herramientas apropiadas y políticas bien trazadas que les permita enfrentar nuevas amenazas. (Impacto Políticas de ciberseguridad, s.f.)

De acuerdo a los acontecimientos de los últimos años, empresas como ABAST han decidido generar nuevas soluciones y servicios para empresas, donde involucran el uso de la Inteligencia de Negocios para la toma de decisiones, algunas de ellas pueden ser usadas en el ambiente de la ciberseguridad y mejorar la seguridad de la información, infraestructura y demás activos de la empresa. Las soluciones como Business Analytics, Minería de Datos, BI Governence son soluciones que, si se utilizan en seguridad, podrían prevenir nuevas vulnerabilidades o amenazas hacia las empresas, sea en empresas privadas, públicas, especialmente de corte financiero.

3.4-Objetivo Específico N° 4.

Determinar las amenazas que pueden esconderse o camuflarse entre grandes volúmenes de datos, que no sean fáciles de detectar con medios convencionales.

Ubicación Geográfica y alcance.

La investigación de las amenazas se realiza a nivel nacional e internacional y comprende los reportes que al momento se han publicado respecto de estudios estadísticos de este fenómeno.

Identificación de variables/ categorías a utilizar en el proceso investigativo.

Las variables identificadas son las siguientes:

- Taxonomía de las amenazas.
- Análisis de amenazas.

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

Los métodos, herramientas e instrumentos que se utilizan para la investigación, son básicamente los siguientes:

- Investigación documental
- Investigación de campo.

Desarrollo de la Investigación

- **Taxonomía de las amenazas**

La GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-400) de España, establece la siguiente taxonomía de las amenazas que afectan a la información:

- Interrupción: genera la pérdida, inutilización o no disponibilidad de la información.
- Interceptación: genera el acceso de un actor no autorizado a la información.
- Modificación: causan la alteración no autorizada de la información; un caso especial es la destrucción, entendida como modificación que inutiliza la información.
- Fabricación: aquellas que tratan de crear información similar de forma que sea difícil distinguir entre la versión original y la fabricada.

La taxonomía de las amenazas, establece que la protección de la información es una mezcla de tres elementos: costes, funcionalidad y protección y vinculan varios aspectos como:

- Análisis de Riesgos: estudio de los riesgos existentes y valoración de las consecuencias de los mismos sobre los activos de información.
- Gestión de Riesgos: valoración de los diferentes controles (elementos que reducen el riesgo) y decisión sobre los más adecuados en cada caso. Esto permite determinar el riesgo residual.
- Política de Seguridad: adaptación de la operativa habitual de la Organización a las medidas de seguridad requeridas.
- Mantenimiento: control permanente de la eficiencia de las medidas de seguridad desplegadas y adecuación de las mismas a nuevos escenarios de riesgo.

- Planes de Contingencia: determinación de las medidas a adoptar ante un incidente de seguridad.

- **Análisis de amenazas.**

Para realizar un análisis de amenazas, se debe comenzar por su definición, que sería la ocurrencia de uno o más eventos de los que se deriva una situación en la que la información puede sufrir una degradación de su seguridad en cualquiera de sus dimensiones: confidencialidad (acceso, difusión, observación, copiado, robo), integridad (modificación, sustitución, reordenamiento, distorsión) o disponibilidad (destrucción, daño, contaminación, dejar fuera de servicio).

Las amenazas van desde desastres naturales, tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos o virus, con un origen tanto interno como externo de una entidad u organización.

Las vulnerabilidades son parte de un sistema de información, por lo que también es necesario conocer su definición. Vulnerabilidad se considera como una debilidad en la seguridad de un entorno que puede llegar a permitir o facilitar la actuación de una amenaza; las vulnerabilidades pueden ser de naturaleza técnica, procedimental u operacional. Habitualmente, en el ámbito TIC, la vulnerabilidad suele ir asociada a un defecto en el software o en la configuración del mismo que puede permitir que se materialice una amenaza.

Para garantizar la confianza de la información, se propone servicios de seguridad que han sido resultado de la aplicación de varios mecanismos de seguridad como:

- Autenticación: permiten al receptor de un mensaje estar seguro de la identidad del emisor y que la comunicación es auténtica. Asegura que el usuario y la información transmitida son auténticos.
- Control de Accesos: protege los recursos del Sistema contra su utilización no autorizada. Los servicios de control de acceso están íntimamente ligados a los de autenticación.
- Confidencialidad: evita el acceso no autorizado a la información, protegiéndola de revelaciones deliberadas o accidentales no permitidas.

- Integridad: protege los datos de alteraciones no autorizadas, detectando cualquier modificación, inserción, eliminación o retransmisión. Comprueba que la información no ha sido modificada sin autorización.
- No Repudio: previenen que la entidad emisora y receptora nieguen haber enviado o recibido un mensaje. Cuando se recibe un mensaje no sólo es necesario poder identificar de forma unívoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que haya podido enviar. En este sentido, es fundamental impedir el repudio, es decir, la negativa por parte de una entidad de haber participado en una comunicación o parte de ella.

Las PYMES según investigación de CISCO, son las empresas más vulnerables. Esto se debe a que estas empresas usan menos procesos de análisis de seguridades y menos herramientas para la defensa de su infraestructura e información, por lo que existen retos en su protección. Además, al ser empresas con pocas personas, no cuentan con un responsable para la seguridad de la información, es decir, que hacen una seguridad de carácter general y por su disponibilidad de recursos económicos, no acceden a servicios de consultoría u otros que les permitan evaluar su situación de seguridad y optar por soluciones, que en la mayoría de los casos son costosas.

Tabla 1
Amenazas

<i>Amenazas</i>	<i>Descripción</i>
<i>DDOs</i>	(Distributed Denial of Service) son una forma relativamente sencilla y efectiva de hacer caer a una Web.
<i>Botnets</i>	Son redes de ordenadores que se emplean para realizar ataques, envíos masivos de correo basura y espionaje contra empresas. Un botnet se crea infectando ordenadores sin que sus propietarios lo sepan.
<i>Malware</i>	Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.
<i>ransomeware</i>	Es un tipo de programa que restringe el acceso a determinadas partes o archivos del sistema infectado.
<i>Archivos Binarios</i>	Son aquellos que contienen información codificada en binario con el propósito de almacenamiento y procesamiento en ordenadores, pueden contener amenazas cifradas.

(Cisco, 2016)

3.5-Objetivo Específico N° 5.

Establecer la forma en la que se puede detectar comportamientos inusuales en el ciberespacio en grandes volúmenes de datos, que pueden constituirse como amenazas cibernéticas, sus mecanismos de defensa y determinar el estado actual de BI en Ecuador referido a la ciberseguridad.

Ubicación Geográfica y alcance.

La investigación de la detección de comportamientos inusuales se realiza a nivel nacional e internacional y comprende los reportes que al momento se han publicado respecto de estudios estadísticos de este fenómeno.

Identificación de variables/ categorías a utilizar en el proceso investigativo.

Las variables identificadas son las siguientes:

- Mecanismos de defensa.
- BI en Ecuador (Encuesta nacional)

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

Los métodos, herramientas e instrumentos que se utilizan para la investigación, son básicamente los siguientes:

- Investigación documental
- Investigación de campo.

Desarrollo de la Investigación

- **Mecanismos de Defensa**

Big Data se utiliza para la predicción de amenazas, puede ser la clave para que las empresas tengan mejor seguridad de la información, realiza la extracción de varias partes de texto, datos, números letras que después de su análisis se transforma en conocimiento y es usado para la toma de decisiones. (Data). Los expertos citan varios ejemplos del uso de Big Data para la predicción de ataques o atentados en diferentes partes del mundo. No solamente se podría determinar predicciones de ataques terroristas sino ataques informáticos, protección de la información que se envía de un lugar a otro. Big Data es un portafolio completo

donde se puede tener beneficios para toma de decisiones relacionadas con la seguridad de la información en las organizaciones.

El objetivo de usar Inteligencia de Negocios en el área de seguridad es obtener un informe ejecutivo de los riesgos, vulnerabilidades de la información y del negocio. De acuerdo a la información recopilada se puede determinar herramientas o soluciones que permitan mitigar las amenazas a la seguridad.

Intel propone un servicio de registro común a gran escala (CLS), un motor de correlación en tiempo real y varias plataformas de análisis personalizadas para ofrecer detección y respuesta más rápidas a las amenazas de seguridad. Recibe muchos eventos y realiza su calificación, proporcionando información y conocimiento de las amenazas que podría tener la empresa. Realiza un análisis y un reporte ejecutivo de las amenazas de seguridad que la entidad podría tener.

Conjuntamente con las herramientas o soluciones que pueden ser usadas para mitigar las amenazas descritas anteriormente, se debe establecer políticas de seguridad. La política de seguridad se considera como una declaración de intenciones de alto nivel, que se ejecutará mediante un desarrollo normativo basado en:

- Procedimientos.- Se establece un marco común de actuación en los procesos de valoración y acreditación de las TIC y cualquier otro campo que se considere.
- Instrucciones Técnicas.- Se considera como un objetivo de seguridad específico. Son de obligatorio cumplimiento en su ámbito de actuación y establecen los requisitos de seguridad generales a implementar en un sistema.
- Normas.- Son reglas generales que se deben seguir o a las que se deben ajustar las conductas, tareas o actividades de las personas y entidades en relación con la protección de la información cuando es manejada por un sistema. Estas normas establecerán las directrices para la redacción de la documentación de seguridad, la realización de análisis de riesgos.
- Guías.- Son recomendaciones o informaciones relativas a temas concretos de seguridad de los sistemas. Estas guías establecerán las configuraciones

mínimas de seguridad de los diferentes elementos de un Sistema, recomendaciones de uso u otro tipo de recomendaciones.

- **BI en Ecuador (Encuesta nacional)**

A continuación, se presenta la evaluación de resultados de la encuesta realizada a nivel nacional respecto de la situación de BI en empresa e instituciones públicas y privadas.

- **Pregunta 1.- Uso de técnicas de investigación y herramientas de Inteligencia de Negocios**

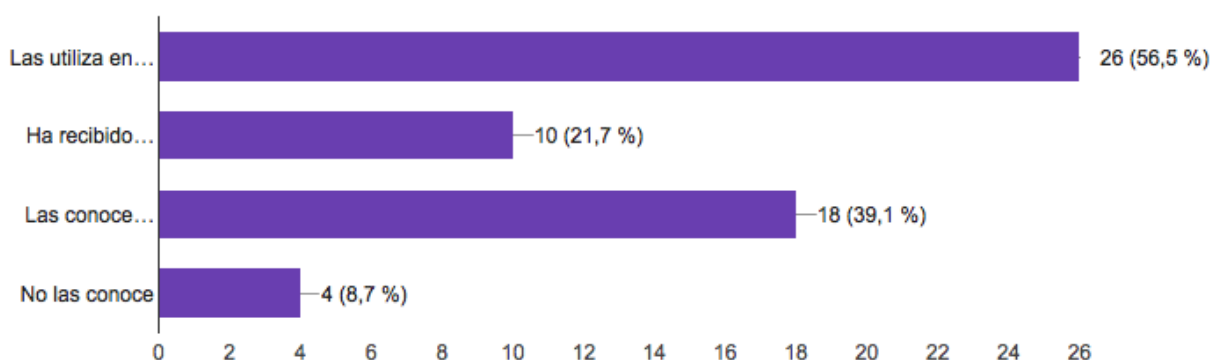


Figura 6 Resultados de la Pregunta 1

Se puede concluir que 26 personas, representantes del 56,5% de la población utiliza en su trabajo herramientas de investigación y soluciones de inteligencia de negocios, el 39,1% en cambio las conoce solamente por referencia, así como diez personas, con el 21,7% de la población ha recibido entrenamiento para el uso de las mismas y un 8,7 % no conoce herramientas de investigación y soluciones de inteligencia de negocios.

- **Pregunta 2.- En el caso de utilizar herramientas de Inteligencia de Negocios, seleccione el tipo de herramienta**

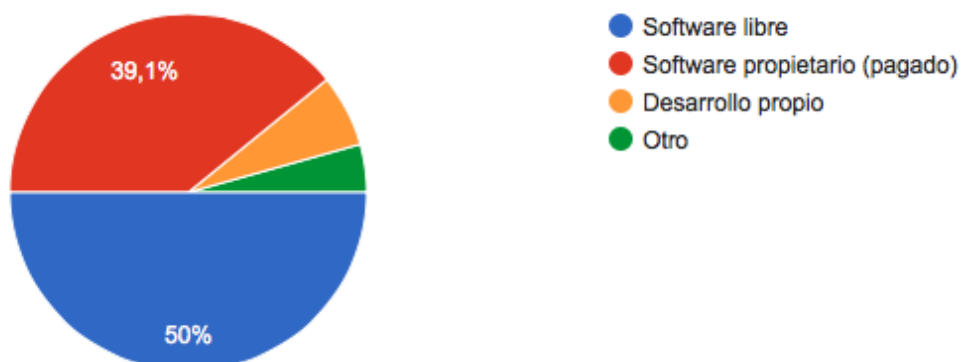


Figura 7 Resultados de la Pregunta 2

De acuerdo a las respuestas obtenidas, se puede concluir que el 50% de la población usa herramientas de software libre, mientras que un 39,1% usa software propietario. Adicional, se pudo obtener que un 6,5% de la población realiza desarrollo de herramientas de BI y el 4,3% restante usa otro tipo de herramientas.

- **Pregunta 3.- ¿Si ha utilizado una herramienta de Inteligencia de Negocios (BI), con qué objetivo lo ha hecho? (señale todas las opciones válidas)**

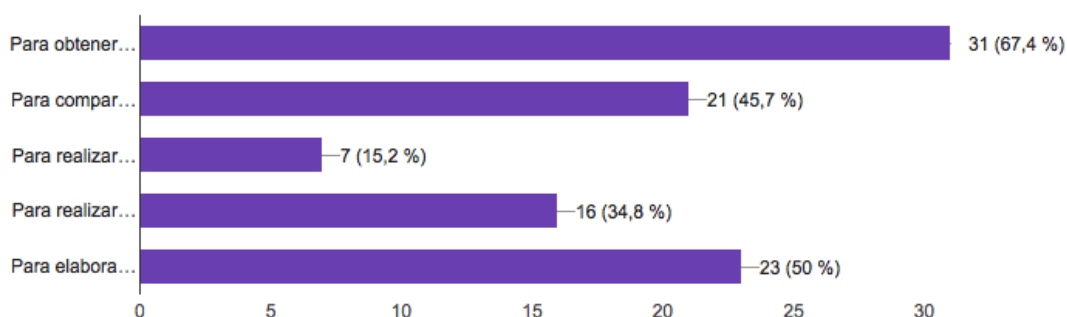


Figura 8 Resultados de la Pregunta 3

La mayoría de personas ha utilizado herramientas de Inteligencia de negocios con el objetivo de obtener datos estadísticos, el 67,4% de la población, mientras que un 50% ha usado estas para elaborar reportes de cumplimiento, también se puede rescatar que un 45,7% usa estas herramientas para comparar datos estadísticos, así como un 34,8% los usa para realizar análisis económico o de negocio. Finalmente, un 15,3% usa herramientas de BI para la realización de investigación de fraudes.

- **Pregunta 4.- Su empresa o entidad, ¿ha elaborado políticas internas para el uso de herramientas de BI?**

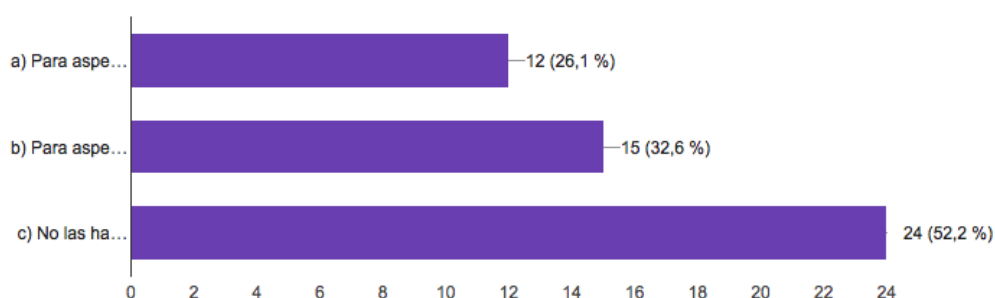


Figura 9 Resultados de la Pregunta 4

Se concluye que el 52,2% de la población no ha elaborado políticas internas de uso de herramientas de inteligencia de negocios, así como el 32,6% ha elaborado políticas de uso de herramientas para aspectos relacionados con el giro del negocio, mientras que un 26,1% restante ha realizado políticas internas para aspectos relacionados con la seguridad informática.

- **Pregunta 5.- Respecto de un sistema de correlación de eventos en su organización (SIEM)**

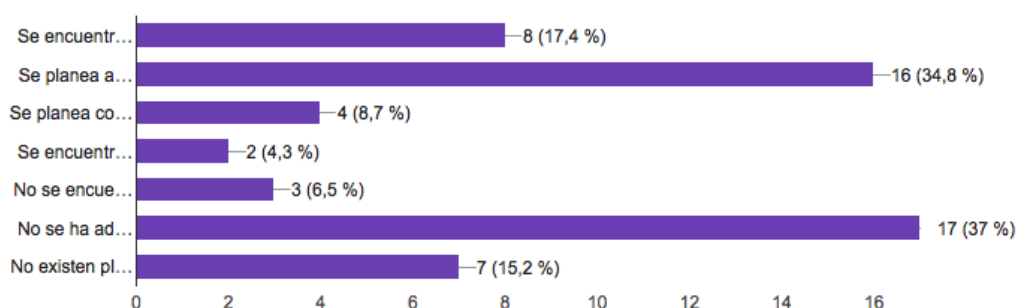


Figura 10 Resultados de la Pregunta 5

Se concluye que un 17,4% de la población ha adquirido un SIEM, sin embargo, la mayoría de empresas planea adquirir en los años posteriores (34,8%). También, se puede constatar que un 8,7% planea contratar un servicio o adherirse a él, teniendo respuesta a incidentes Informáticos. Adicional, en la minoría de las empresas, se dice que tienen un SIEM pero que sus resultados no son significativos para ellos. Un 6,5% tienen un sistema de correlación de eventos pero no lo usan, pero lo más alarmante es que la gente de TI no ha adquirido un y representa un 37% de la población.

Finalmente, existe empresas, un 15,3%, que piensa que no hay necesidad de adquirir uno o ni si quiera se encuentra en planes de colocar un sistema parecido.

- **Pregunta 6.- Cree usted que las herramientas o soluciones de BI serían una ayuda para:**

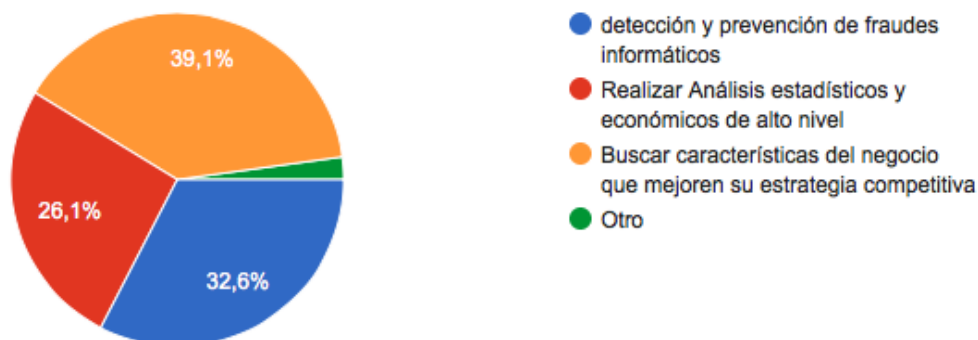


Figura 11 Resultados de la Pregunta 6

Se concluye que la gran mayoría de las personas, un 39,1% de la población, cree que las herramientas o soluciones de BI serian de ayuda para buscar características del negocio que mejoren su estrategia competitiva, pero también el 32,6% de la población concuerda que sería de gran ayuda para la detección y prevención de fraudes informáticos. También, un 26,1% cree que sería de ayuda para realizar análisis estadísticos y económicos de alto nivel y finalmente, un 2.2% se usaría para otros fines.

- **Pregunta 7.- Para utilizar adecuadamente herramientas de BI en seguridad de la Información se debería (señale las opciones válidas en prioridad):**

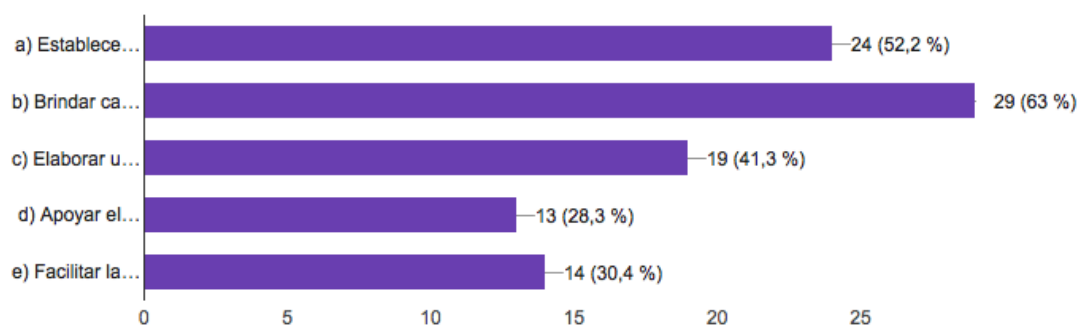


Figura 12 Resultados de la Pregunta 7

Para el uso de herramientas o soluciones de BI para la seguridad de la información, el 63% de la población cree que es necesario brindar capacitación y difundir su uso, así como también un 52,2% piensa que establecer una política nacional de ciberseguridad ayudaría a su uso y explotación. Sin embargo, un 41,3% de la población cree que elaborar un programa nacional para la difusión de esta tecnología permitirá crecer el uso de las herramientas o soluciones de BI. Adicional, el 28,3% Apoya el uso de software libre relacionado y el 30,4% piensa que se debería facilitar la adquisición de software relacionado.

- **Pregunta 8.- ¿Cuál cree que sería la principal dificultad para utilizar herramientas de BI en su negocio?**

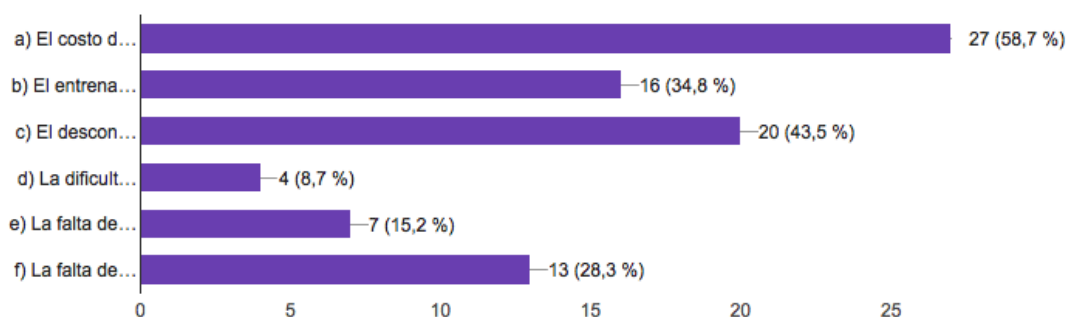


Figura 13 Resultados de la Pregunta 8

Claramente se concluye que la barrera de adquisición de una herramienta o solución de BI es el costo de la misma, eso opina el 58,7% de la población, sin embargo, el desconocimiento por parte de las autoridades sobre las bondades que proporciona esta tecnología también viene a formar parte de la falta de adquisición de herramientas, esto representa un 43,5%. Así también la falta de entrenamiento necesario de las soluciones, hace que las personas no exploten en su totalidad a la solución o herramienta, opina el 34,8%, adicional, la falta de formación relacionada de los técnicos informáticos hace que sea una dificultad también, representado por el 28,3%. Se concluye, que la falta de un soporte técnico a estas soluciones, también se una dificultad en su uso, piensa el 15,2%. Finalmente, la dificultad de uso de las herramientas o soluciones de BI, solo representan el 8,7% de la población, es decir, que las herramientas o soluciones son amigables para el usuario.

- **Pregunta 9.- Las autoridades de su institución, ¿están conscientes de los riesgos en la seguridad de la información y cómo mitigarlos?**

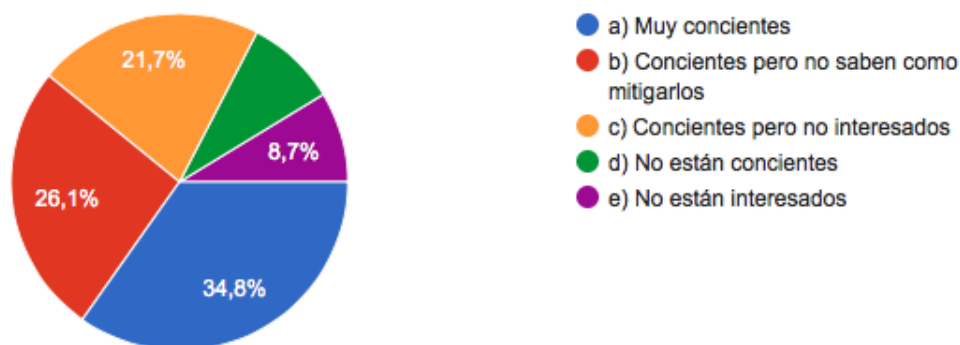


Figura 14 Resultados de la Pregunta 9

Se concluye que en su mayoría, 34,8% de la población, son muy conscientes sobre los riesgos en la seguridad de la información, sin embargo, el 26,1% piensa que son conscientes, pero no conocen la forma de mitigar dichos riesgos. Sin embargo, un 21,7% de las autoridades son conscientes, pero no están interesados y finalmente un 17,4% se comparte entre no conscientes y no interesados.

- **Pregunta 10.- Si el Estado desea crear una Política Nacional de Ciberseguridad podría usted:**

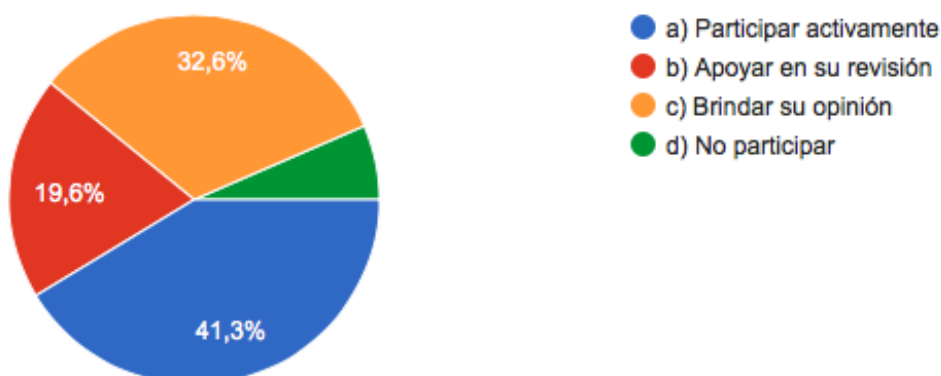


Figura 15 Resultado de la Pregunta 10

Se concluye que un 41,3% participaría activamente en la creación de una política nacional de ciberseguridad, así como el 32,6% brindaría una opinión constructiva para

la misma. Adicional, un 19,6% puede apoyar en la revisión y un mínimo de 6,5% no participaría.

- **Conclusión final.**

Se puede concluir finalmente y en relación a la Hipótesis presentada inicialmente en este estudio, que con la encuesta realizada, se puede comprobar que efectivamente que en el Ecuador no se cuenta con políticas de ciberseguridad específicas, en forma definida y permanente, sea en entidades públicas como privadas y peor aún aquellas que empleen métodos de Inteligencia de Negocios en su apoyo, como se puede ver es incipiente el uso de estas herramientas tan útiles tecnológicamente en la prevención y mitigación de amenazas y riesgos en el país.

La elaboración de Políticas Nacionales y su aplicación, por tanto se convierten en una verdadera necesidad, como hacerlo, es tema del trabajo del Ing. Mario ron en su tesis doctoral, pero en ellas debe constar lo relacionado al uso de BI en la ciberseguridad.

CAPÍTULO 4.- PROPUESTA

4.1. Justificación de la Propuesta

Los ciberdelicuentes buscan países con bajos estándares o estrategias de seguridad en el ciberespacio, para instalar redes y bases de operaciones para sus organizaciones, que pueden ser físicas o virtuales. Esto representa una problemática no solo a nivel de país sino que puede tener efectos sociales y económicos en otros países y como tal se debe enfrentar estas amenazas, en consecuencia es necesario formular una Política Nacional de Ciberseguridad que desde una perspectiva de política pública incorpore en sus procesos críticos niveles de seguridad en el ciberespacio según estándares internacionales y de esta manera incorporar al Ecuador a los organismos que internacionales preocupados de crear políticas para mejorar la vida de sus poblaciones.

Una política de ciberseguridad es necesaria por las siguientes razones:

- Proteger la seguridad de las personas en el ciberespacio.- El principal objetivo de un estado es la protección de los derechos fundamentales de las personas, especialmente aquellos que dicen relación con sus interacciones en el ciberespacio.
- Salvaguardar la seguridad del país.- Es fundamental resguardar las redes y sistemas informáticos del sector público junto a aquellos componentes del ciberespacio.
- Causar la colaboración y coordinación entre instituciones.- Los elementos involucrados en la ciberseguridad se encuentran segmentadas de acuerdo a diversos criterios, por lo tanto, promover la colaboración, coordinación y sinergia de todos los organismos involucrados en la seguridad en el ciberespacio llegaría a crear mejoras.
- Administrar los riesgos del ciberespacio.- La ciberseguridad contempla el desarrollo de un proceso de análisis y gestión de riesgos relacionados con la identificación de vulnerabilidades y amenazas, originando así un análisis de riesgo por cada entidad para la prevención de nuevas amenazas y vulnerabilidades.

4.2. Ejes de una Política Nacional de Ciberseguridad relacionada con BI.

Los ejes que se exponen a continuación en la Tabla 2, agrupan varias medidas que de acuerdo a estándares internacionales, suelen utilizarse en el marco de políticas de ciberseguridad y que son necesarios de acuerdo a la realidad nacional:

Tabla 2
Ejes de una Política de Ciberseguridad

Eje	Descripción
Infraestructura de la información	Gestión de riesgo. Identificación de infraestructura crítica. Prevención y sanción. Mecanismos de incidentes. Definición de estándares. Diseño de planes de contingencia.
Prevención y Sanción	Aumento de capacidades para investigar cibercrímenes Diseño de mecanismos de resguardo Establecimiento de desafíos en prevención, detección y sanción de cibercrímenes.
Sensibilización, formación y difusión	Fomento de la investigación y desarrollo Promoción de la cultura en ciberseguridad Promoción de la capacitación
Cooperación y relaciones internacionales	Participación en foros nacionales e internacionales Asistencia internacional
Institucionalidad de la ciberseguridad	Revisión del sistema nacional de ciberseguridad Definición de roles, atribuciones y competencias Intercambio de información Fomento en el uso de herramientas de BI para la prevención de amenazas y vulnerabilidades

4.3. Funciones e institucionalidad necesarias para desarrollar una Política Nacional de Ciberseguridad relacionada con BI.

Para crear una política nacional de ciberseguridad y siguiendo el ejemplo de aquellos países que han participado en este proceso hace algunos años, resulta indispensable para Ecuador contar con una entidad pública que desempeñe las funciones que se identifican como esenciales.

Por esta razón, es necesario la creación de una entidad pública, que se relacione con el Poder Ejecutivo a través de algún ministerio y que cuente con personal de carrera, responsable de la ejecución de funciones específicas relacionadas con la ciberseguridad de la Nación y un consejo superior de ministros que defina las orientaciones políticas y ejerza las facultades normativas necesarias para su correcto funcionamiento. El personal involucrado deberá tener la formación y el conocimiento sobre la ciberseguridad y actividades relacionadas.

Las funciones que se identifican como esenciales se representan en la figura 17:



Figura 16 Funciones que la entidad debe cumplir

Las instituciones intervinientes en materia de ciberseguridad y que podrían integrar un Consejo relacionado a este tema, a nivel nacional, se representan en la figura 18.



Figura 17 Entidades intervinientes

- **Ministerio del Interior:** Garantiza la seguridad ciudadana y convivencia social pacífica en el marco del respeto a los derechos fundamentales, la democracia y la participación ciudadana con una visión integral que sitúa al ser humano en su diversidad como sujeto central para alcanzar el Buen Vivir.
- **Ministerio de Defensa:** Como órgano político, estratégico y administrativo, diseña y emite políticas para la Defensa y administración de las Fuerzas Armadas, a fin de garantizar y mantener la soberanía e integridad territorial; así como, apoya al desarrollo nacional con su contingente.
- **Ministerio de Telecomunicaciones y sociedad de la información:** Órgano rector del desarrollo de las tecnologías de la información y comunicación en el Ecuador, que incluyen las telecomunicaciones y el espectro radioeléctrico, que emite políticas, planes generales y realiza el seguimiento y evaluación de su implementación, coordinando acciones con los actores de los sectores estratégicos para garantizar el acceso igualitario a los servicios y promover su

uso efectivo, eficiente y eficaz, que asegure el avance hacia la sociedad de la información para el buen vivir de la población ecuatoriana.

- **Ministerio de Finanzas:** Contribuye al cumplimiento de los objetivos de desarrollo del país y a una mejor calidad de vida para las y los ecuatorianos, a través de una eficaz definición, formulación y ejecución de la política fiscal de ingresos, gastos y financiamiento público; que garantice la sostenibilidad, estabilidad, equidad y transparencia de las finanzas públicas.
- **Ministerio de Relaciones Exteriores y Movilidad:** Rector de la política internacional y responsable de su gestión y coordinación, de la integración latinoamericana y la movilidad humana, respondiendo a los intereses del pueblo ecuatoriano, al que rinde cuentas de sus decisiones y acciones en cumplimiento de los principios constitucionales y de las normas del derecho internacional, en el marco de los planes nacionales de desarrollo.
- **Universidad de las Fuerzas Armadas:** Facilitador técnico-científico, responsable de proponer soluciones a nivel nacional, tanto para entidades públicas como privadas y promover el conocimiento en el área, con programas de formación y capacitación y proyectos de investigación y vinculación que permitan aplicar las Políticas Nacionales.
- **Servicio Ecuatoriano de Normalización:** Organismo técnico nacional, eje principal del Sistema Ecuatoriano de la Calidad en el país, competente en Normalización, Reglamentación Técnica y Metrología, que contribuye a garantizar el cumplimiento de los derechos ciudadanos relacionados con la seguridad; la protección de la vida y la salud humana, animal y vegetal; la preservación del medio ambiente; la protección del consumidor y la promoción de la cultura de la calidad y el mejoramiento de la productividad y competitividad en la sociedad ecuatoriana.
- **Ministerio de Justicia, Derechos Humanos y Cultos:** Vela por el acceso a una justicia oportuna, independiente y de calidad, promueve la paz social, la plena vigencia de los Derechos Humanos, el ejercicio de cultos y su regulación, mejora la rehabilitación y su reinserción social en las personas adultas privadas

de libertad y el desarrollo integral en adolescentes en conflicto con la ley penal, mediante normas, políticas, programas, proyectos y actividades coordinadas con las instituciones relacionadas.

El trabajo mancomunado de estas instituciones permitirá el desarrollo de una política nacional de ciberseguridad, adecuada a la realidad del país, con las regulaciones respectivas, así como estrategias que brinden soluciones a esta problemática que aqueja a la seguridad de la información en el mundo.

4.4. Esquema Gubernamental de Seguridad de la Información (EGSI)

La sociedad exige que la información sea adquirida, procesada, almacenada y transmitida por medios confiables y seguros, ello ha motivado a las organizaciones y empresas a configurar esquemas que brinden confianza en el uso de las TIC, por eso es importante referirse a este modelo que integra todos los elementos necesarios para cumplir con esos requerimientos.

- **Misión**

Establecer lineamientos de seguridad informática y protección de la infraestructura computacional, mediante políticas, normas, estrategias, procesos, procedimientos y tecnologías.

- **Funciones o responsabilidades principales**

- Proponer o designar un comité de seguridad de la información, un oficial de seguridad de la información y una entidad para la auditoría de cumplimiento y evaluación de los riesgos.
- Ofrecer asesoramiento experto sobre seguridad en redes y sistemas de información a las autoridades nacionales, ministerios, subsecretarías, intendencias, gobernaciones e instituciones estatales de importancia crítica.
- Funcionar como agente de control y regulación para la implementación de buenas prácticas.
- Facilitar el contacto entre las instituciones estatales, autoridades nacionales y empresas privadas de infraestructuras críticas.
- Desarrollar planes de recuperación ante desastres (DRP).
- Proponer la actualización de leyes sobre ciber-delitos.

- Apoyar a las Pymes en temas de seguridad de la información, debido que son las más propensas a ser intervenidas por los ciber-delincuentes.
- Desarrollar el capital humano, para lograr la excelencia operativa en distintas áreas estratégicas, a través de cursos referentes a las últimas amenazas de la información y la forma de protegerse.
- Promover el uso adecuado de redes sociales en colegios, empresas privadas, empresas públicas y entidades bancarias.
- Desarrollar e implementar un plan de Inteligencia Cibernética con la finalidad de coordinar todas las actividades para detectar, disuadir y mitigar las amenazas de inteligencia interna y externa a los sistemas de información de Ecuador.
- Participar en convenios internacionales para realizar investigaciones que permitan la detección de ciberdelincuentes, formando parte de una estrategia de Defensa Cibernética que evite interferencias en la justicia internacional y logre también desarrollar capacidades de monitoreo y respuesta.
- Desarrollar un centro criptológico nacional, para el desarrollo y generación de mecanismos avanzados de seguridad, normas y estándares que permitan al país lograr la independencia tecnológica en cuanto al resguardo de información sensible.
- Desarrolla de normas de seguridad de la Información de Salud, Bancario, Casas de Valores y otras, en las que se contemple sanciones respecto del incumplimiento de la normativa.
- Desarrollar un marco de trabajo para la mejora de ciberseguridad de infraestructura crítica
- Proteger los derechos de las personas naturales y jurídicas, propiciando sus libertades civiles en relación a la seguridad de la información tomando en cuenta que se deberá:
 - ✓ Incentivar el acceso de los usuarios a las tecnologías de cifrado.
 - ✓ Evitar el diseño o la implementación de "puertas traseras" (backdoors) o vulnerabilidades en herramientas, tecnologías o servicios.

- ✓ Fortalecer, mejorar los estándares de cifrado e influir intencionalmente en su desarrollo, para promover un mayor nivel de seguridad de la información.
- ✓ Exigir algoritmos, estándares, herramientas o tecnologías de cifrado seguros.
- ✓ Apoyar el uso de herramientas de Software Libre de Inteligencia de Negocios para la mitigación de amenazas.
- ✓ Impedir por acuerdo privado o público, que las personas entidades actúen de manera incompatible con estos principios.

CAPÍTULO 5.- CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La Inteligencia de Negocios es un conjunto de técnicas, procesos y herramientas que permiten tomar decisiones para el negocio, a través del uso de patrones, sin embargo, se puede también prevenir amenazas y mitigar riesgos, utilizándola en ciberseguridad.
- En el Ecuador, no existen al momento políticas de ciberseguridad en las que se considere Inteligencia de Negocios, puesto que las empresas usan herramientas o soluciones de la misma para fines estadísticos y referentes al crecimiento del negocio, pero en forma muy incipiente en labores relacionadas con la seguridad de la información.
- Las amenazas cibernéticas han crecido de manera significativa, por el uso cada vez mayor de la Internet, que conduce al incremento del riesgo a la seguridad de la información. Esto ha obligado al desarrollo de técnicas y métodos de análisis de las vulnerabilidades y amenazas por medio de herramientas de BI inteligentes que permiten prevenir y mitigar el efecto de nuevos delitos informáticos.
- Existen mecanismos de defensa para prevenir delitos informáticos, que han sido aplicados por muchos países, uno de ellos es crear políticas nacionales de ciberseguridad referidas a BI, que permitan establecer una hoja de ruta acoplada a las tendencias mundiales en la seguridad de la información y brinden confianza en el uso de TIC.

5.2.Recomendaciones

- Propiciar el uso de la tecnología relacionada con Inteligencia de Negocio, especialmente patrones de comportamiento de actividades inusuales, para fortalecer los esquemas gestión de la seguridad de la información.
- Apoyar la elaboración y aplicación de políticas de ciberseguridad en las que se considere Inteligencia de Negocios, para que en las empresas e instituciones se utilice no solamente con fines estadísticos y referentes al crecimiento del negocio, sino en labores relacionadas con la seguridad de la información.
- Difundir el conocimiento de las amenazas cibernéticas, así como el de técnicas y métodos de análisis de las vulnerabilidades y amenazas por medio de herramientas de BI inteligentes que permiten prevenir y mitigar el efecto de nuevos delitos informáticos.
- Participar en la elaboración de una Política Nacional de Ciberseguridad, que al igual que otros países de la región permita establecer una hoja de ruta acoplada a las tendencias mundiales en la seguridad de la información, que brinde confianza en el uso de TIC.
- Considerar los resultados de la encuesta realizada, para trazar una línea de base en cuanto al uso de BI en ciberseguridad.

BIBLIOGRAFÍA

- (s.f.). Obtenido de Universidad Politécnica de Madrid:
<http://www.upm.es/Investigacion/AyudasConvocatorias>
- (s.f.). Obtenido de INCIBE: <https://www.incibe.es>
- (s.f.). Obtenido de <http://confseguridad.upb.edu/programa/leyes/>
- A. Magela, R. A. (s.f.). *ACADEMIC ANALYTICS: APLICANDO TECNICAS DE BUSINESS INTELLIGENCE SOBRE Palavras-Chave Palabras Clave.*
- Astigarraga, E. (2006). *El metodo Delphi.*
- Baumgartner, R. F. (2005). Web data extraction for business intelligence: the lixta approach. *In Proc. of BTW 2005*, 30-47.
- Cisco. (2016). Informe Anual de Seguridad.
- Data, B. (s.f.). *Huffingtonpost*. Obtenido de http://www.huffingtonpost.ca/2015/11/12/big-data-public-safety-security_n_8541376.html
- Deloitte. (s.f.). Obtenido de <http://es.slideshare.net/roberth.chavez/seguridad-informtica-en-el-ecuador-expreso-v18082011>
- E. Antonio, R. A. (2013). *Representación visual de patrones de ataque en ciberseguridad.* San José, Costa Rica: ULACIT.
- E. Antonio, R. A. (s.f.). *Representacion visual de patrones de ataque en ciberseguridad.*
- E. Leiva, P. M. (2015). *Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Vision Local* (Vol. 3).
- Fiscalía. (s.f.). Obtenido de <http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje.html>
- G. Mondrag, C. G. (s.f.). *Revision Sistemática de Literatura: Visualización de Seguridad.*
- Golfarelli, M. R. (Noviembre de 2004). Beyond data warehousing: what's next in business intelligence?. In Proceedings of the 7th ACM international workshop on Data warehousing and OLAP. *ACM*, 1-6.
- Impacto Políticas de ciberseguridad.* (s.f.). Obtenido de <http://100seguro.com.ar/europa-analiza-el-impacto-de-las-politicas-de-ciberseguridad-y-la-prevencion-de-datos/#sthash.ihKmQO4z.dpuf>
- ISACA. (s.f.). *Definiciones.*
- J. Carrillo Ruiz, F. C. (2013). *Big Data en los entornos de Defensa y Seguridad.*
- J. Eom, N. K. (2012). *Cyber military strategy for cyberspace superiority in cyber warfare.*
- J. LoroseMe, R. P. (2015). *No Title* (Vol. 1).
- Krause, M. (1995). *La investigacion cualitativa: Un campo de posibilidades y desafios* (Vol. 7).
- L. Jimenez, S. H. (s.f.). *Enfoque Sociotecnico Aplicado a un Sistema de Gestion Business Intelligence.*
- L. JIMENEZ, S. H. (s.f.). *Enfoque Sociotecnico Aplicado a un Sistema de Gestion Business Intelligence.*
- L. Niu, J. L. (2008). *Intelligent Decision and Policy Making Support Systems.*
- Lavado de Dinero.* (s.f.). Obtenido de <http://es.slideshare.net/danielamariacepedaaguilar/lavado-de-dinero-en-ecuador>
- Leyes de Seguridad Informática.* (s.f.). Obtenido de Seguridad InformáticaCiclo de Conferencias y Mesas Redondas: <http://confseguridad.upb.edu/programa/leyes/>
- Leyes y Regulaciones.* (s.f.). Obtenido de <http://dennisvill.blogspot.com/2012/05/leyes-y-regulaciones-sobre-los-delitos.html>

- Mosso, J. (2015). *Ciberseguridad Inteligente*.
- Negash, S. (2004). *Communications of the Association for Information Systems Business Intelligence BUSINESS INTELLIGENCE*.
- Políticas de conectividad a las TIC desde un enfoque de derechos. Especial atención al caso de Ecuador Políticas de conectividad a las TIC desde un enfoque de derechos.* (s.f.).
- R. Wetzker, T. A. (2007). *An Unsupervised Hierarchical Approach to document categorization*.
- Ramos, M. (2014). *CENAE Acerca de la soberanía del Ecuador en el ciberespacio*.
- Richards, K. (s.f.). *SearchDataCenter En Español*. Obtenido de TechTarget: <http://searchdatacenter.techtarget.com/es/cronica/Nuevos-patrones-de-seguridad-emergen-para-la-analitica-de-grandes-datos>
- S. BARRENTO, M. N. (2010). *Sistemas de Business Intelligence Aplicados a Saude. Selección preliminar de tendencias en Ciberseguridad Estudio de tendencias en Ciberseguridad*. (2016).
- SophosLabs. (s.f.). Obtenido de <https://www.sophos.com/en-us/threat-center/threat-analyses.aspx>
- T. Mahmood, U. A. (2013). *Security Analytics: Big Data Analytics for Cybersecurity*.
- Vión, J. F. (s.f.). *Blog NEO*. Obtenido de <http://www.indracompany.com/es/blogneo/retociso-ciberespacio>
- W. Yeoh, A. K. (2010). *Critical Success Factors for Business Intelligence Systems*.
- Wikipedia. (s.f.). Obtenido de <http://www.wikipedia/ciberseguridad.com>
- Y.A.A. (2010). *La seguridad, ciberseguridad.retos y amenazas a la seguridad nacional en el ciberespacio*.
- Yorio. (2006). *Identificación y clasificación de patrones en el diseño de aplicaciones móviles*. Argentina: RD.

ANEXOS

ANEXO A- ENCUESTA

CUESTIONARIO PARA INVESTIGACIÓN DE CAMPO

Dirección de correo electrónico *

- 1. Respecto de las técnicas de investigación y herramientas de Inteligencia de Negocios ***
 - Las utiliza en su trabajo
 - Ha recibido entrenamiento para su uso
 - Las conoce por referencia
 - No las conoce
- 2. En el caso de utilizar herramientas de Inteligencia de Negocios, seleccione el tipo de herramienta. ***
 - a) Software libre
 - b) Software propietario (pagado)
 - c) Otro:
- 3. ¿Si ha utilizado una herramienta de Inteligencia de Negocios (BI), con qué objetivo lo ha hecho? (señale todas las opciones válidas) ***
 - a) Para obtener datos estadísticos Para comparar datos estadísticos Para realizar investigación de fraudes
 - b) Para realizar análisis económicos o de negocio
 - c) Para elaborar reportes de cumplimiento (requeridos por entidades de control)
- 4. Su empresa o entidad, ¿ha elaborado políticas internas para el uso de herramientas de BI? ***
 - a) Para aspectos relacionados con la seguridad informática
 - b) Para aspectos relacionados con el giro del negocio
 - c) No las ha elaborado
- 5. Respecto de un sistema de correlación de eventos en su organización (SIEM) ***
 - a) Se encuentra adquirido
 - b) Se planea adquirir
 - c) Se planea contratar un servicio o adherirse a él (Respuesta a Incidentes Informáticos)
 - d) Se encuentra en uso pero su servicio no es significativo No se encuentra en uso
 - e) No se ha adquirido
 - f) No existen planes o necesidades de adquisición
- 6. Cree usted que las herramientas o soluciones de BI serían una ayuda para: ***
 - a) detección y prevención de fraudes informáticos
 - b) Realizar Análisis estadísticos y económicos de alto nivel
 - c) Buscar características del negocio que mejoren su estrategia competitiva
 - d) Otro:
- 7. Para utilizar adecuadamente herramientas de BI en seguridad de la Información se debería (señale las opciones válidas en prioridad): ***
 - a) Establecer una política nacional de ciberseguridad
 - b) Brindar capacitación y difundir su uso

- c) Elaborar un programa nacional para la difusión de esta tecnología
 - d) Apoyar el uso de software libre relacionado
 - e) Facilitar la adquisición de software relacionado
- 8. ¿Cuál cree que sería la principal dificultad para utilizar herramientas de BI en su negocio? ***
- a. El costo de las herramientas
 - b. El entrenamiento necesario
 - c. El desconocimiento por parte de las autoridades de las bondades de esta tecnología
 - d. La dificultad de su uso
 - e. La falta de empresas nacionales que brinden soporte
 - f. La falta de formación relacionada de los técnicos informáticos
- 9. Las autoridades de su institución, ¿están conscientes de los riesgos en la seguridad de la información y cómo mitigarlos? ***
- a. Muy conscientes
 - b. Conscientes pero no saben cómo mitigarlos
 - c) Conscientes pero no interesados
 - c. No están conscientes
 - d. No están interesados
- 10. Si el Estado desea crear una Política Nacional de Ciberseguridad podría usted: ***
- a. Participar activamente
 - b. Apoyar en su revisión
 - c. Brindar su opinión
 - d. No participar

HOJA DE LEGALIZACIÓN DE FIRMAS

**ELABORADA(O) POR
ANDREA ESTEFANÍA VACA HERRERA**

Srta. Ing. Andrea Vaca Herrera

COORDINADOR DE LA MAESTRÍA

Sr. Ing. Germán Ñacato

Lugar y fecha: Diciembre del 2016