República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

UTEG Facultad de Estudios de Postgrados

Tesis en opción al título de

Magister en: MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Tema de Tesis:

Medir el Impacto que contribuye las vulnerabilidades en los sistemas Financieros, Fiscalía al Momento de dar un Balance de las debilidades de cómo se desarrollan los Crímenes Cibernéticos, su Resultado Nefasto En La Economía Del Ecuador

Autor:

Lic. Patricia E. Rodas Soto, Abg.

Director de Tesis

Phd. José Towsend

Enero 2021

Guayaquil – Ecuador

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Graduación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la **"UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL".**

(Reglamento de Graduación de la UTEG)

_____

Lic. Patricia E. Rodas Soto

CI. 0920633393

DEDICATORIA

Agradecerle a Dios por esta etapa que culmina a mis padres, familia por siempre estar presente en cada meta trazada para realizar este logro el seguir adelante cada y alcanzar los objetivos necesarios.

El motor de cada día para alcanzar metas y sueños es para mi hija que tenga un aliciente de que cuando tenga que alcanzar un sueño lo logre con esfuerzo y dedicación

Con esfuerzo y dedicación para todos los que creyeron en mí.

Patricia Estefanny Rodas Soto

AGRADECIMIENTO

Este proyecto de grado le agradezco a cada persona que de una u otra manera me ayudo para poder realizarlo ya que no era fácil de construir cada parte de el con su colaboración y ganas de contribuir con este pequeño estudio

Mi agradecimiento a la Universidad Tecnológica Empresarial de Guayaquil, alma máter donde tuve la oportunidad de adquirir nuevos conocimientos para ser aplicados en mi entorno laboral y profesional.

En especial agradecer al Doctor José Townsend Director y Tutor de tesis, Docente universitario por su ayuda, consejos, conocimientos y experiencia; sobre todo por su valioso tiempo dedicado a este trabajo de tesis.

Y agradecer a cada dos de mis compañeros del área a Mildred y Alfredo que me ayudaron en este camino de elaboración con su ayuda y colaboración con datos en esta meta trazada.

Patricia Estefanny Rodas Soto

RESUMEN

En esta investigación se busca evaluar la aplicación de un modelo de seguridad de la información para la medición de los delitos informáticos y su incidencia en la toma de decisión estratégica en la Fiscalía General del Estado. Como objetivo principal se busca caracterizar un modelo de la seguridad de la información para la toma de decisiones estratégica ante las vulnerabilidades del sistema financiero y la realización de los crímenes cibernéticos. La metodología empleada es cualitativa, el nivel de la investigación es descriptivo, no experimental y transversal. La principal conclusión es la mejora en la toma de la decisión estratégica a la hora de implementar un sistema de gestión ISO27001 ante los delitos informáticos a las personas y al sector económico del estado ecuatoriano.

Palabras claves: Normas ISO 27001, delito informático, riesgo Informático, seguridad de la información.

ABSTRACT

This research seeks to evaluate the application of an information security model for measuring cybercrime and its impact on strategic decision-making in the State Attorney General's Office. The main objective is to characterize an information security model for strategic decision-making in the face of vulnerabilities in the financial system and the carrying out of cyber-crimes. The methodology used is qualitative, the research level is descriptive, non-experimental and transversal. The main conclusion is the improvement in making the strategic decision when implementing an ISO27001 management system in the face of computer crimes to the people and the economic sector of the Ecuadorian state.

Keywords: ISO 27001 standards, computer crime, computer risk, information security.

Indicé

Índice de Tablas

Índice de Gráficos

Índice Cuadros

Anexos

Figuras

Introducción

En la investigación realizada se aborda el tema de los delitos informáticos y como la fiscalía general del estado trata estos riesgos informáticos con una metodología que es un muy poco convencional con el mundo de hoy. Estos delitos en el ámbito de los sistemas financieros han sido manejados de que si se comete este tipo de desvió de fondos, las pruebas deben ser manipuladas por la fiscalía bien incautando el equipo.

Dentro de la en los delitos informáticos en el Ecuador han sido unos de los mayores índices delictivos en los últimos años desde el 2014 hasta la actualidad, es por ello que al realizar el análisis de casos de apropiación fraudulenta a través de medios electrónicos es imprescindible dar a conocer que los casos de fraude, estafa, robo de claves contraseñas, son comunes en el diario vivir.

En este estudio, se observará como parte del desarrollo del proyecto un modelo de seguridad de la información código penal ya lo tipifican el delito Informático como tal, en Ecuador al haber entrado en vigencia el COIP, desde el 2019 se han dado innumerable caso algunos de ellos quedan en la impunidad, debido a que no se continua con la causa. Es decir, el hecho como de apropiarse de números de cuentas contraseñas para ingresar. Es por ello que se dará a conocer que la propuesta es factible a través de la investigación realizada, de los elementos argumentativos de cómo se desarrolla el hurto, dentro y fuera de las instituciones financieras en el país aplicando el modelo ISO27001.

En las conclusiones de este proyecto tenemos que se pudo cuantificar los delitos informáticos, las pérdidas de los bancos versus el como como mejoraría los ingresos de las utilidades cuando se estructure buen sistema de planificación de riesgos en su mayor parte con resultados que ayuden a la economía procesal, tiempos, resultados que permitan al usuario afectado el hecho de recuperar lo robado a través de los medios electrónicos que hayan

sido susceptibles de interceptación ilegal de los datos, que no solo causan molestias si no que es un abuso, al esfuerzo que cada usuario hace para poder guardar sus dineros, el tramite eterno solo para que se demuestre que hubo el robo, fuga de datos desde la entidad financiera. La principal conclusión es la mejora en la toma de la decisión estratégica a la hora de implementar un sistema de gestión ISO27001 ante los delitos informáticos a las personas y al sector económico del estado ecuatoriano.

Capítulo I. Marco Teórico Conceptual

1.1. Antecedentes de la investigación

Con el paso del tiempo la tecnología y la criminalística forense han dado a conocer con el paso de los años. Pero, no ha tenido un avance fructífero para detener, mejorar y cuantificar el avance de los delitos informáticos con diversos tipos de delitos tales como en empresas dedicadas al sector financiero, comercial. Estos han presentado diversos tipos de problemas de ataques informáticos.

Con ello, perjudicando la economía de empresas privadas y públicas. Las mismas que no se han dado estos problemas recientes, si no desde la creación de las redes sociales que desde allí empezaron los ataques informáticos, y las diversas formas de hurtar, clonar, obtener datos de otra persona. Como resultado, es un perjuicio a las empresas por no administrar el buen uso de la tecnología que ha ido en aumento con el avanzar de los años. Y con ella, el progreso del software.

En referencia a dicho problema en el año 2019 la revista primicias en su artículo publicado se desarrolla el mayor porcentaje de los delitos informáticos, como es el delito de apropiación fraudulenta por medios electrónicos que se encuentran tipificados en el Código Orgánico Integral penal (Fiscalia, 2019).

En los porcentajes los cuatro delitos más comunes están se hallan (ver gráfico 1):

- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones
- Ataque a la integridad de sistemas informáticos
- Revelación ilegal de base de datos
- Interceptación ilegal de datos

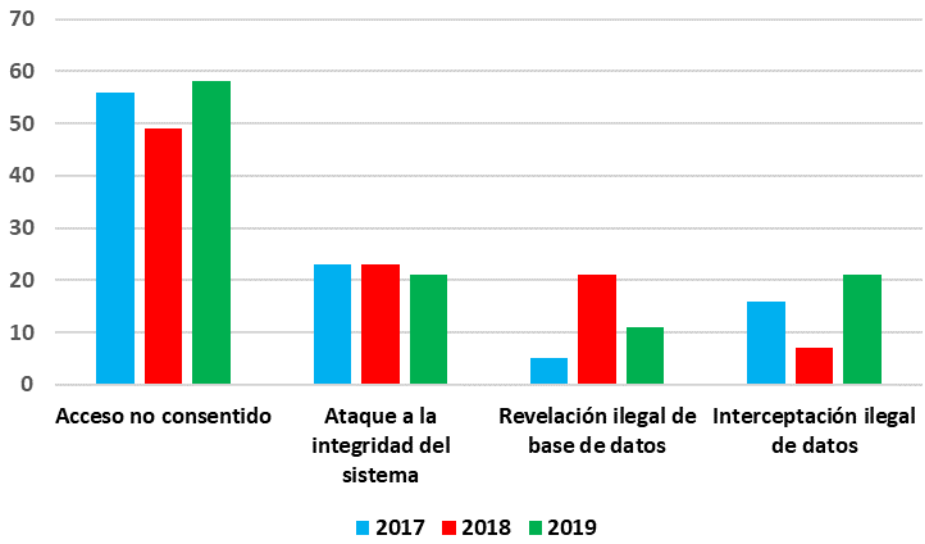


Gráfico 1. Incidencia de los delitos cibernéticos más comunes (2017-2019)
Fuente: Elaboración propia según *(Interior, 2019)*

Según Bayardo &Santacruz (Hugo Bayardo Santacruz1, 2019), no solo en Ecuador se ha dado perdidas económicas por estos delitos, es por ello que la Comisión Económica para América Latina y el Caribe (CEPAL) estableció que en América Latina, el 45,5% de los hogares tiene acceso a internet, de estos hogares que tienen mayor acceso de conectividad como Costa Rica, Uruguay y Chile, con cifras mayores al 56%; mientras que en países como Ecuador, Perú, Colombia, Venezuela, México, entre otros, su porcentaje está entre el 15% y 45%.

Entonces, en el recuento de los delitos informáticos nos hace falta una buena cultura tecnológica a los ecuatoriano, para tener un rápido y mejor avance tecnológico en el país con seguridad, que se encarguen de los ingresos de la banca electrónica, a nivel mundial personas inescrupulosas, maliciosas y con amplios conocimientos informáticos realicen actos que vulneren los derechos de otras personas por medio de internet (Vera, 2019).

Por lo tanto, los actos que son dirigidos contra la confidencialidad e integridad de los sistemas informáticos que han sido vulnerados y que no han sido considerados a la medida. Estos se han detectado como son el número total de casos de ataques cibernéticos resueltos, en proceso. De la misma manera en qué lugares son los que con mayor frecuencia se dan. Para ello, con el

desarrollo de este aplicativo se podrá contabilizar y dar una mejor expectativa de los delitos informáticos en la provincia del Guayas. Según encuestas aplicadas por el **INEC** la mayor cantidad de delitos informáticos se encuentra en la ciudad de Guayaquil, provincia del Guayas, luego sigue la ciudad de Quito, provincia del Pichincha.

Como resultado, la aplicación de una metodología de gestión, la cual disminuiría significativamente los riesgos de calidad de software. No obstante, nunca se alcana el 100% en cuestión de calidad. También, el uso de los mismos tiene sus desventajas: alarga el tiempo de un proyecto, obliga a llevar documentación detallada del mismo durante su ejecución.

Para mejorar la situación financiera del país las entidades bancarias analizan medidas de protección para el usuario. La importancia del estudio de los delitos informáticos y las medidas de prevención protegen a todo usuario de fraudes y robos que surgen por medios electrónicos (Ajila, 2019).

1.2. Planteamiento del problema de investigación

De acuerdo a las investigaciones realizadas en la Fiscalía General del Estado una de las principales causas de la desconfianza de la banca electrónica por los usuarios es el hecho de los elevados casos de delitos informáticos como son los de OLA BINI, entre otros delitos de apropiación fraudulenta que han conmocionado al país, pero el tener un mejor control de crímenes cibernéticos.
Los más polémicos según investigaciones realizadas desde el 2019, en la fiscalía de patrimonio ciudadano son los delitos de cuello blanco los cuales son prácticamente imperceptibles para los usuarios de los sistemas interconectados en la banca virtual.

Por ello que en las investigaciones realizadas en la Fiscalía de Patrimonio ciudadano se dan a conocer a diario múltiples tipos de delitos informáticos tipificados en el COIP, con una figura no muy clara, para los hackers, crackers, phrikers, quienes tienen una identificación de características claras en las que

trabajan para sustraer información, clonar páginas web, tarjetas de crédito o débito.

Sin lugar a dudas el solo tipificar con la característica de delito por medio electrónico como apropiación fraudulenta, en ocasiones no solo es cuestión de que un agente extraño tome información, tarjetas de débito o crédito; si no también los silenciosos los mismos funcionarios de los bancos, de alguna institución comercial.

Para poder resolver el hecho de que el tiempo de investigación y de una de principales causales de que se investigue los delitos informáticos es la falencia en los tiempos de dar resultados, que estos delitos sean sancionados según lo establece la ley en el menor tiempo posible, con un modelo de seguridad de la información aplicado en la fiscalía y que se realice la auditoria informática en tiempo que a futuro permita al usuario al denunciar a tiempo cada una de los atropellos que puede sufrir en la web.

1.2.1. SÍNTOMAS

- Falta de control en los tiempos de ejecución de la Fiscalía (CSA, 2011).
- Falta de seguridad y privacidad para de parte de la Fiscalía en los procesos ejecutados (Gonzales, 2016).
- Falla de los servicios y aplicaciones de denuncia agiles y seguras para los usuarios (Joyanes, 2009).
- Falta compromiso con el usuario para la devolución de su pérdida de dinero en línea (Mieres, 2009).

1.2.2. CAUSAS

- Injerencia de ataques informáticos en los sistemas financieros.
- Sistemas financieros no toman precauciones en contra d las

vulnerabilidades, tecnología obsoleta.

- No se da el soporte técnico necesario para poder evitar las intromisiones de ataques cibernéticos.
- Ingeniería social.

1.2.3. PRONÓSTICO

- Pérdida de dinero en línea, clonación de tarjetas, o claves.
- Modelo de seguridad de la información y accesos vulnerados.
- Controlar los servicios con un modelo de sistemas información, para los servicios en línea.
- Denuncia de usuarios.

1.3. Formulación del problema

¿Se podrá evaluar la aplicación de un modelo de seguridad de la información para la medición de los delitos informáticos y su incidencia en la toma de decisión estratégica en la Fiscalía General del Estado?

1.3.1. Sistematización del problema

- ¿Será necesario la existencia de un modelo de seguridad de la información ISO 27001 para el control de los delitos informáticos?
- ¿Podrá ser indispensable la seguridad, la protección y la rapidez para solución de delitos informáticos por parte de para Fiscalía General?
- ¿Puede existir mejoría en el proceso de resolución de las denuncias por delitos informáticos aplicando modelo ISO 27001?
- ¿Es posible que la Fiscalía General del estado pueda identificar ataques informáticos, y evitar los delitos económicos a las personas y al estado?

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Caracterizar un modelo de seguridad de la información para la toma de decisiones estratégica ante las vulnerabilidades del sistema financiero y la realización de los crímenes cibernéticos.

1.4.2. Objetivos específicos

- Definir los sustentos teóricos, jurídico, metodológico y práctico para el desarrollo de un modelo de seguridad de la información y la medición de los delitos informáticos en la Fiscalía General del Estado.
- Cuantificar los ataques cibernéticos y defraudación al sistema financiero y economía en general receptados por la Fiscalía General del Estado
- Catalogar los ataques informáticos ejecutados al sistema financiero por los delincuentes informáticos receptados por la Fiscalía General del Estado.
- Recomendar un modelo de sistemas de información basado en las normas de calidad ISO 27001 para la medición de los delitos informáticos para la Fiscalía General del Estado, en Ecuador.

1.4.3. Justificación de la investigación

Conveniencia:

El aplicar la tecnología en el ámbito jurídico para mantener la relevancia y potencia administrativa será de ayuda y contribuirá en el desarrollo de funcionarios con mayor calidad jurídica, educativa, administrativa, ya que dará una mejor visión de los delitos informáticos que en nuestro país no es tomado en consideración ya que los toman como delitos menores en el código integral penal.

Relevancia social:

Los fundamentos de la investigación son la globalización del desarrollo tecnológico y los cambios en la forma de educar, socializar y abrir campo en el ámbito jurídico para de manera asincrónica el estado evaluar maneras que se manifiesta el delito informático en la población y la economía del estado.

Aplicaciones prácticas:

La necesidad de adoptar un enfoque novedoso para mejorar el tratamiento de los datos, brindando una solución de Inteligencia de negocio que pueda dar apoyo a la toma de decisiones empresariales, implementando nuevas estrategias de negocio enfocadas a la creación de información inteligente a partir de los datos almacenados.

Aporte metodológico:

La presente investigación pretende generar conciencia en los beneficios al adoptar prácticas enfocadas al aprovechamiento del Big data y uso de herramientas de inteligencia de negocio, brindado así un ágil proceso de gestión de los datos generando diferentes soluciones de los reportes realizados por CIB (banca de inversión) y con ello suspender las deficiencias presentadas en el área en cuanto a tiempos, informes, estrategias de negocio y por ultimo resaltar la importancia que tienen los datos en el negocio, buscando presentar al lector una visión más amplia que permita identificar oportunidades de aplicabilidad a nivel empresarial.

1.5. Marco de referencia de la investigación

1.5.1. Marco teórico

El entorno del ciberataque

Según M. Uma y G. Padmavahi (2013) determinaron que los ciberataques se han convertido en una diario vivir para todas la empresas en general que buscan espacios en la red para poder generar ingresos a sus arcas atacando a

través se amenazas y vulneraciones en la red que no han permitido el mejorar las economía de diversas empresas (Padmavathi, 2013).

A todas estas se desarrollan una inexplicable comprensión de diversos tipos de ataques que contienen características, estos resultados le pueden ayudar para mantener la defensa de seguridad de la información. Según varios autores en términos técnicos se podría definir el término de ciberataque, ciberdelincuencia, que tendrán el mismo objetivo como es confidencialidad, integridad y que la disponibilidad de los datos este para que se verifique que hay intromisiones en la web.

1.6. Delito Informático

Según, el Código Orgánico Integral Penal tipifica algunos delitos que, según las denuncias receptadas en la Fiscalía General del Estado, han sido los más denunciados con respecto a la vulneración de sistemas informáticos. Los cuatro delitos informáticos con mayor número de denuncias son:

- El acceso no consentido a un sistema informático, telemático o de Telecomunicaciones (tipificado en el artículo 234)
- El ataque a la integridad de sistemas informáticos (artículo 232)
- La interceptación ilegal de datos (artículo 230)
- Revelación ilegal de bases de datos (artículo 229)

De esta manera, el COIP expresa que estas contravenciones pueden ser sancionadas con la privación de la libertad de tres a cinco años. En la revista científica de estudio en la de los delitos en el mundo como Novaestrat, se tomó la información digital de que prácticamente todos los ecuatorianos han sido vulnerados sus bases de datos e información personal que, donde se ofrecen servicios de marketing digital e inteligencia de mercados.

Según, un informe de una de las famosas consultoras Deloitte donde explica el acceso a esta información, donde miles de ecuatorianos han sido perjudicados, por la vulneración a su privacidad como es parte del robo de identidad,

clonación de claves de acceso, duplicado de tarjetas de crédito entre otras tipos de vulneraciones son parte del espionaje comercial. (Dávila, 2019)

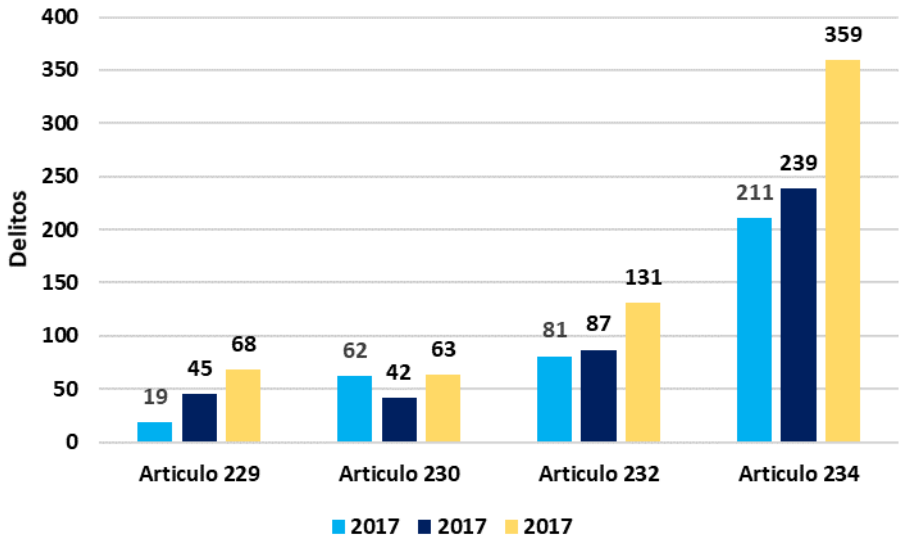


Gráfico 2. Delitos Informáticos por Artículos del COIP
Fuente: Elaboración propia según Revista Primicias

Los delitos informáticos se inician en los años 60s que le ha dado el origen desde el almacenamiento de los datos personales en las computadoras, en el año de 1984 George Orwell, realizaba el control y vigilia de las personas atravesó de las tecnologías lo cual dio pie a este tipo de delitos por primera ocasión (Zumárraga., 2002).

Como detalle de los ciberdelito que es un acto ilícito que se comete con una computadora o un celular que son las herramientas más comunes de tener un alto índice robo de información, clonaciones de tarjetas, duplicidad de claves entre otros (Aggarwal & Arora , 2014).

También, el delito cibernético como tal es un acto totalmente ilegal y es uno del punto clave en el cual la tecnología de información y comunicación se han visto afectadas. (Yahma, 2015). “La evidencia nos muestra que organizaciones como bancos, agencias gubernamentales, instituciones de salud y grandes corporaciones que mantienen datos de gran valor tienen más probabilidades de

ser atacadas con más frecuencia que la mayoría" (Global_Cybersecurity_Report, 2017).

1.6.1. Tipos de atacantes

Para identificar los delitos informáticos o ataques cibernéticos debemos vivirlos en 3 categorías específicas:

- El delincuente informático con una motivación financiera que quiere apropiarse de los sistemas y realizar robos o fraudes electrónicos.
- Este personaje espía para poder robar la información, y dársela a un tercero.
- El delincuente informático se encuentra motivado y es la manera de comprometer la información o sistemas (Pettersson, 2012).

1.6.2. Instituciones Financieras

Es por que entre las instituciones financieras que se han realizado investigaciones se ha dado a conocer son intermediarios en los mercados bursátiles y que tienen gran productividad (Siklos, 2001). Una institución bancaria de ahorro o prestamos, o mutualista, depósitos e inversiones (Swanda, 2010).

1.6.3. Ataques Cibernéticos en las Instituciones Financieras

En definiciones de los ataques cibernéticos, el observatorio económico y productivo de la ESPOCH, con sede en la ciudad de Morona Santiago realizó una investigación de los avances tecnológicos, uso de herramientas digitales son parte de la vida cotidiana que han desarrollado varios antecedentes de existencia de ataques a entidades financieras (RAMÍREZ, 2019).

Dentro de las mismas se han podido verificar la naturaleza del riesgo a detectar

un riesgo de fraude informático tal cual lo manifiestan varios autores acerca del mismo que ha sido uno de los principales, amenazas o vulnerabilidades (Jankalová, & Jankal, 2017), (Štitilis, Pakutinskas, & Kinis, 2016), (Allabouche & Diouri, 2016) y (Baronienė & Žirgutis, 2017).

Para estos autores el fraude es uno de los principales delitos informáticos que causan vulnerabilidades y amenazas constantes. Estos grupos criminales son profesionales que se encuentran bien resguardados y se desarrollan a nivel nacional e internacional con la tecnología de punta para atacar las redes de las organizaciones financieras (Čirjevskis, 2016).

Para las organizaciones financiaciones el fraude se realiza sin su consentimiento que la información estratégica que debería estar resguardada no lo está, los bancos al cuidar las bases datos, con grandes cantidades de información pueden ser extraídas por los datos almacenados (Munteanu & Tamošiūnienė, 2015).

En un caso real de un fraude informática con las tarjetas de crédito o pago debe tener dos clase de identificación como las transacciones de fraudulentas (Maes, Tuyls, & Vanschoenwinkel, 2002).

Según Bhatla y col. (2003) se argumenta que debido a una tarjeta de crédito puede ser clonada, robada y para ello tiene tres categorías (Bhatla , Prabhu, & Dua, 2003):

- Fraude tradicional con tarjetas (tarjetas robadas, solicitud de tarjeta, adquisición, imitación y cuentas falsas).
- Fraude relacionado con el negocio (colusión y triangulación de distribuidores).
- Fraude relacionado con Internet (clonación de sitios, generación de tarjetas de crédito y sitios de comerciantes falsos).

Un caso de vital importancia, la transacción con tarjetas de pago puede tener lugar en cuestión de minutos, pero los efectos secundarios del fraude a través

de líneas telefónicas o comunicaciones electrónicas pueden continuar durante meses, a veces años, en forma de procesos legales largos y costosos (Štitilis, D; Klišauskas, V, 2015) (Kriviņš, 2015).

Es decir que la seguridad económica y financiera personal puede verse principalmente como una cuestión de decisión personal y sentido común (Baronienė & Žirgutis, 2017). En la actualidad, es el fenómeno de la globalización y la diversificación, el que se está volviendo dominante, y hasta tal punto que la mayoría de sujetos económicos actúan de acuerdo con lo que se denomina “desatención racional” (Button, 2008).

Al mismo tiempo, la deuda personal y la libertad económica se han convertido en elementos clave de todas las (Kriviņš, 2015). El proceso de seguridad se centra en el riesgo operativo definido como un riesgo de pérdida resultante de procesos internos o fallas de capital humano o de condiciones externas (Pettersson, 2012).

La seguridad de los clientes es el factor clave del éxito de los bancos. El factor mencionado influye mucho en la adquisición, retención o pérdida de clientes. Por esa razón, es decisivo que un banco comercial adopte tales medidas para garantizar una protección adecuada y eficiente de los clientes (Aggarwal & Arora , 2014).

La situación actual exige que los bancos comerciales presten una atención extraordinaria a la seguridad de las tarjetas de pago. El cumplimiento de las necesidades y requisitos de los consumidores (Siklos, 2001), la satisfacción de los clientes bancarios y la atención integral al cliente están hoy en día en el centro de atención de investigadores y banqueros.

Según Maes, Tulys y Vanschoenwinkel (2002) varios investigadores están tratando de encontrar las principales motivos que el cliente tiene para dar su visto bueno de satisfacción con la bancar y examinar estos temas desde

diversas perspectivas (Maes, Tuyls, & Vanschoenwinkel, 2002).

Las redes, los emisores, los adquirentes y los reguladores, han desempeñado sus respectivos roles en la gestión eficaz del fraude en los pagos, contribuyendo así en gran medida al rápido crecimiento de la adopción de los pagos electrónicos por parte de los consumidores (Munteanu & Tamošiūnienė, 2015).

Las industrias y los negocios las tecnologías de información son indispensables, debido a que el tráfico transaccional de las organizaciones ha aumentado considerablemente lo cual ocasiona inconvenientes en el control de las actividades realizadas mediante plataformas virtuales (Granda, 2020).

Entonces, las organizaciones gubernamentales y empresas financieras siguen siendo el objetivo principal de muchos ciberataques, tales como extorsión, robo, fraude, suplantación de identidad, entre otros.

Para tratar el fraude electrónico se lo relaciona íntimamente con la transformación a nivel digital que vivimos en un mundo globalizado, y esto ha afectado al ámbito financiero que es difícil de comprender o de conceptualizar como se perpetra el fraude financiero y que toma la tecnología como un delito informático, desde un punto de vista técnico-informático según la normativa nacional (GONZÁLEZ, 2017).

1.6.4. Riesgo cibernético y por qué es relevante para la estabilidad financiera

Para el instituto de gestión de riesgos lo define como un peligro que una organización se encuentre desprotegida en vulnerabilidades informáticas y que tengas pérdidas significativas por algún tipo de falla de sus sistemas tecnológicos de información (Hathaway, 2018).

Los ataques cibernéticos tienen un tinte de tipo malicioso de beneficio en este caso los hackers vulneran los accesos restringidos para dañar, hurtar, obstruir todo tipo daño a los sistemas digitales de cualquier organización dominarlo, o robar la información que se tenga- (Ramírez, 2017).

1.6.5. Principales ataques cibernéticos a Instituciones Financieras

Los principales ataques cibernéticos a continuación se detallan:

- **Malware**

Para definir lo que es un malware es un programa que se creó con la intención de robar datos, dañar equipos, en general este software se lo utiliza para que se reproduzcan los llamados virus malware informáticos, gusanos, troyanos, rootkits, adware, spyware (Gavilánez, 2017).

El malware puede incluir virus y cualquier otro software malicioso, no deseado cuyo comportamiento es no deseado; y una degradación del rendimiento del sistema, ya que la infección puede crear actividad del procesador, uso de memoria y tráfico de red no deseados (Stahlberg, 2009).

- **Phishing**

Se lo conoce También como fraude informático se usa como medio de ingeniera social el cual se basa a reacciones humanas; engaña al usuario con nombres, usuarios, contraseñas, números de tarjetas de crédito o débito de manera ilícita o fraudulenta (Lux, 2020).

Para (Siklos, 2001) uno de los autores de la teoría o concepto de Phishing, se lo contextualiza que el mismo puede dirigir sus ataques a usuarios a sitios web fraudulentos. En pocas palabras, el Phishing se ha convertido en una

amenaza. Estos ataques de suplantación de identidad en los correos electrónicos y sitios web de apariencia legítima son falsos engañan a los usuarios para que revelen información personal o financiera al atacante. (Minn Wu, 2019).

- **Ataque BIN**

En tanto el termino BIN es una secuencia de los 6 primeros números en las tarjetas de crédito. Es necesario tener esta secuencia, la fecha de expiración para realizar la estafa. Se pueden usar más números para generar números válidos (Burgos, 2005).

Las pérdidas de las industria bancaria en todo el mundo debido a delitos de cuello blanco como este son enormes y superan con creces los métodos convencionales de robo bancario (Dashtana, 2013).

- **Rounding Down o Técnica del Salami**

Esta técnica consiste en el desvió de pequeñas cantidades de dinero de cuentas con montos altos, al igual que un salami al cortarlo en rodajas muy pequeñas, este no sufre una reducción considerable y así esta acción pasa completamente inadvertida, generalmente se atacan equipos Unix los cuales se utilizan para operaciones financieras.

Un ejemplo es el redondeo de divisas es un ataque que no recibe mucha atención, pero se ve mucho. Es decir, el redondeo de divisas es la capacidad de tomar una falla en el código de computadora y hacer que el esfuerzo de redondeo del software funcione a favor del atacante (Štitilis, Pakutinskas, & Kinis, 2016). El banco generalmente redondeará hacia arriba o hacia abajo para completar la conversión (Yahma, 2015). El redondeo ocurre al número más cercano. Las personas que realizan un ataque de redondeo de divisas (Stahlberg, 2009).

- **Skimming o clonación de tarjetas**

Este método consiste en la duplicación de tarjetas para su posterior uso delictivo, se presentan en cajeros automáticos modificados, gasolineras, restaurantes, bares en los cuales los dueños se prestan para proveer de esta información obtenida a los delincuentes informáticos. Queda impregnado en la banda magnética, que cuando se haga el deslizamiento de los lectores de tarjetas, estos datos son: fecha de expiración, número de tarjeta, nombre del titular y el número de seguridad que aparece en el reverso de las tarjetas o el CVV (Štitilis, D; Pakutinskas, P; Kinis, U, 2016).

Una práctica ilegal utilizada por ladrones de identidad para capturar subrepticiamente información de tarjetas de crédito de un titular de tarjeta. Los estafadores a menudo usan un dispositivo llamado skimmer que se puede instalar en surtidores de gasolina o cajeros (Štitilis, Pakutinskas, & Kinis, 2016).

- **Ransonware**

El ransomware es una amenaza en rápida evolución contra la que las instituciones financieras de todo el mundo deben estar atentas (Yahma, 2015).

Normalmente este software ataca a organizaciones con información relevante, aparece visitando un sitio web infectado, o incrustado en un documento adjunto de un correo electrónico el cual contiene un troyano. (Čirjevskis, 2016)

- **Ataque Man-In-The-Middle**

También es conocido como ataque de intermediario, este ataque lee, modifica mensajes entre dos personas sin su conocimiento; este fraude roba información del usuario como por ejemplo los datos al realizar una compra online (Kuehl, 2009).

1.6.6. El entorno de La ciber resiliencia

La ciber resiliencia se ha convertido recientemente en uno de los conceptos

más publicitados en las discusiones sobre ciberseguridad, a pesar de, o quizás debido a, su significado nebuloso, lo que dificulta su definición y medición rigurosa. Su popularidad está indudablemente ligada a los numerosos titulares sobre ciberataques y filtraciones de datos que salpican las portadas de periódicos y sitios web de tecnología, anunciando información sobre hackers nuevos y masivos que revelan la fragilidad de nuestras infraestructuras digitales y la incapacidad de las organizaciones para proteger los datos personales que encomendarles. Incluso las organizaciones más conocedoras de la tecnología y conscientes de la seguridad no son inmunes a las fallas catastróficas de ciberseguridad.

Para tomar prestada una metáfora poderosa, las organizaciones, una vez que aceptan el hecho de que operan en un estado permanente de vulnerabilidad cibernética mientras obtienen considerables beneficios de productividad de las tecnologías que también amenazan su existencia, deben aprender a "sobrevivir con una dieta de fruta envenenada" (Danzig , 2014).

En palabras de uno de los padres fundadores del concepto este cambio de perspectiva “no requiere una capacidad precisa para predecir el futuro, sino solo una capacidad cualitativa para diseñar sistemas que puedan absorber y acomodar eventos futuros en cualquier forma inesperada que puedan tomar” (Holling, 1973).
Es importante diferenciar la resiliencia de la gestión de riesgos, aunque están entrelazados. La gestión de riesgos implica la cuantificación de la probabilidad y gravedad de los riesgos, lo que permite respaldar decisiones sobre la estrategia más adecuada para abordarlos, como inacción, evitación, reducción, transferencia o seguro (Button, 2008).

La resiliencia tiene un alcance más amplio y “es esencial cuando el riesgo es incompatible, como cuando las condiciones peligrosas son una completa sorpresa o cuando el paradigma analítico de riesgos ha demostrado ser ineficaz” (Linkov & Eisenberg , 2013). La resiliencia reemplaza a la gestión de riesgos cuando esta última ha sido ineficaz para proteger a una organización de amenazas disruptivas e implica un ciclo constante de actividades y

respuestas, comenzando mucho antes de un evento adverso y concluyendo mucho después de que el evento ha terminado, para implementar la adaptación.

Medidas necesarias para contrarrestar el próximo impacto impredecible. En otras palabras, mientras que la gestión de riesgos en la ciberseguridad se ocupa de la minimización de los peligros, la ciber resiliencia busca mantener altos niveles de rendimiento independientemente de la presencia o ausencia de peligros (Bagheri & Ridley , 2017).

Esto explica por qué “una organización puede tener ciberseguridad sin ser resiliente, pero no al revés. (Bodeau & Graubart, 2011). La necesidad de aplicar el pensamiento y las prácticas de resiliencia al ecosistema digital puede parecer superflua, ya que Internet fue diseñado para ser un elemento resiliente. Sistema distribuido que podría persistir en las peores situaciones posibles, como un ataque nuclear (Castells, 2001).

.

Pero esta capacidad de recuperación técnica, que se limita a una de las capas básicas que constituyen Internet y garantiza que el enrutamiento de paquetes de datos pueda seguir múltiples rutas alternativas (Kuehl, 2009), llegando a los destinatarios incluso si se eliminan una cantidad no trivial de nodos de conexión, nunca fue destinado a proporcionar un nivel confiable de seguridad para un mundo en el que todas las actividades sociales y transacciones comerciales posibles se han migrado en línea, miles de millones de dispositivos están conectados a la web y las personas, los procesos y las políticas son explotados de manera rutinaria y exitosa por actores maliciosos. Dada la escala y gravedad sin precedentes de los riesgos cibernéticos, la resiliencia cibernética debe extenderse más allá de la infraestructura global de Internet, centrándose en cambio en las organizaciones individuales que han llegado a depender de ella para cumplir su función.

1.6.7. Análisis de los datos de bancos e instituciones financieras

En una operación estadística considerada en datos publicados por la Superintendencia de Bancos y por la Superintendencia de Economía Popular y Solidaria. En ambos casos, se publicó información relacionada a las pérdidas de las instituciones financieras por ataques informáticos. Para ello, se adjunta tabla 1.

Tabla 1. *Perdidas de las Instituciones Financieras*

AÑO	BANCO DEL PACIFICO	BANCO PICHINCHA	BANCO DEL AUSTRO	COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO	CACPE PAST	COOPERATIVA NACIONAL	COOPROGRESO	TOTAL PERDIDAS ALCANZADAS POR LAS INSTITUCIONES FINANCIERAS Y COOPERATIVAS DE AHORRO
2017	$237.890,00	$25.101,00	$170.400,00	$200,00	$1.811,00	$225,00	$9.540,00	**$445.167,00**
2018	$196.390,00	$23.658,00	$132.100,00	$789,00	$1.729,00	$145,00	$17.980,00	**$372.791,00**
2019	$178.500,00	$21.632,00	$115.000,00	$356,00	$1.681,00	$230,00	$15.980,00	**$333.379,00**
2020	$155.000,00	$17.856,00	$98.700,00	$236,00	$1.257,00	$254,00	$11.840,00	**$285.143,00**

Fuente: Superintendencia de Bancos y Seguros

Los ataques más comunes se pueden detallar en la siguiente tabla No. 2

Tabla 2*. Tipo de Ataques Informáticos*

LOS ATAQUES MAS COMUNES AL SECTOR FINANCIERO	TIPO DE INSTITUCION FINANCIERA	PERDIDA A LAS INSTITUCIONES BANCARIAS	ESPECIALISTA EN SEGURIDAD
Malware	bancos/cooperativas	25%	ING. EN SISTEMA
Phishing	bancos/cooperativas	25%	ING. EN SISTEMA
Ataque BIN	bancos/cooperativas	25%	ING. EN SISTEMA
Rounding Down o Técnica del Salami	bancos/cooperativas	30%	ING. EN SISTEMA
Skimming o clonación de tarjetas	bancos/cooperativas	30%	ING. EN SISTEMA
Ransonware	bancos/cooperativas	25%	ING. EN SISTEMA
Ataque Man-In-The-Middle	bancos/cooperativas	25%	ING. EN SISTEMA

Fuente: Fiscalía General del Estado

1.7. Modelos de Gestión de riesgos y amenaza para la Seguridad Informática

Para que la Fiscalía general del estado tenga un mejor funcionamiento en cuanto a los procesos que se deben de llevar se va analizar tres modelos que son importantes para poder realizar un estudio de qué modelo se puede usar con mayor efectividad. A continuación, tenemos tres modelos escogidos por su alto potencial de detección de riesgos, vulnerabilidades informáticas:

COSO 2013

En el caso del modelo COSO I 2013, donde se evalúan los riesgos informáticos cuyas características son las siguientes:

- Puede detectar el riesgo con rapidez, pero no implementa medidas seguridad a través de políticas recomendadas para que no vuelva a suceder dicho inconveniente, estos riesgos deben poder mitigarse antes de lleguen a una denuncia, ya que causan conmoción social con la que impacta un riesgo en la entidad, es decir, se refiere al ritmo con el que se espera que la entidad experimente el impacto.
- Cuando hay una amenaza, un riesgo se debe realizar una trayectoria de duración del riesgo el impacto que ha tenido en la sociedad. (Fulss, Marzo).

COBIT 5

Apetito de riesgo

- Las características de Cobit 5 para detección de los riesgos se rige más a nivel directivo en una institución sin tomar en consideración a los mandos medios que son quienes hacen cumplir los objetivos de la organización (ISACA, 2013).
- En este modelo se tolera mucho la variación del riesgo y se lo acepta a nivel gerencial cuando debe ser mitigado y alcanzar un objetivo (ISACA, 2013).
- Capacidad de riesgo al no poder resolver el riesgo de las pérdidas económicas y no continuar la organización (ISACA, 2013).

1.7.1. Normas ISO 27001 de Gestión De Riesgos

Para implementar el modelo ISO 27001 se necesitas los siguientes requisitos dentro de la fiscalía para poder analizar y verificar riesgos y vulnerabilidades:

Requisitos de seguridad

Hay tres fuentes principales a tener en cuenta al establecer los requisitos de seguridad de la información de una organización:

- **Evaluación/análisis de riesgos**: Considerando los objetivos de cada institución, como son las estrategias del negocio, se debe verificar las vulnerabilidades, amenazas en los activos cual sería el impacto del negocio (ver figura 1).
- **Legislación vigente**: Nuestra legislación vigente contiene estatutos, reglamentos que cumplir de acuerdo a la normativa del COIP que permite que tanto la institución como los usuarios tengan protegidos su información.
- **Conjunto de principios:** Estos requisitos de seguridad deben alinearse a los objetivos de la organización, el procesamiento de los datos y sus operaciones.

Figura 1.ISO 27001 Riesgos
Fuente: Guía de ISO 27001

Para obtener mejores resultados de una gestión de procesos en ISO 27001, en la gestión de procesos riesgos tenemos lo siguiente:

- **Selección de controles**

Para seleccionar los controles o medidas para hacerle frente a las

vulnerabilidades, reducir el riesgo de incidentes en la seguridad de la información. Se debe gestionar los riesgos, con las políticas de cada organización procedimientos, directrices, prácticas o estructuras organizativas que pueden ser de carácter administrativo, técnico, de gestión o legal.

- **Control ISO 27001**

Según los controles de la norma NTC ISO/IEC 27002:2007 Y NTC ISO / IEC 27001:2006; se deben de régimen Constitución, ley, regulaciones naciones e internacionales vigentes actualmente para la seguridad de la información y los negocios de la organización. Ejemplos de control de acceso físico:

- Puertas
- Carteles de “prohibido entrar”
- Circuito cerrado de televisión
- Contraseñas
- Controles biométricos
- Las políticas de seguridad
- Manual de responsabilidad
- Antivirus, copias de seguridad
- Control de acceso lógico

1.7.2. Los controles de seguridad de la información

Entre los controles al software que utiliza las empresas se deberán regir a los controles de gestión de riesgo, políticas internas directrices, procesos, prácticas que serán de los procedimientos administrativos, técnico, legal o de gestión. Para ver varios de los controles se darán lo siguiente en la seguridad de la información, como son las organizaciones, con base en requisitos legales y / o mejores prácticas para la seguridad de la información.

En el punto de vista legal, existen controles considerados fundamentales y dependen de la legislación vigente como son:

- Protección de datos y privacidad de la información personal.

- Protección de los registros de la organización

Los controles considerados buenas prácticas para la seguridad de la información son:

- Documento de la política de seguridad de la información.
- Asignación de responsabilidades para la seguridad de la información;
- Sensibilización, educación y capacitación en seguridad de la información
- Procesamiento correcto en las aplicaciones.
- Gestión de las vulnerabilidades técnicas
- Gestión de la continuidad del negocio.
- Gestión de incidentes de seguridad de la información**.**

1.7.3. Gestión de la seguridad de la información Modelo ISO 27001

En cada organización se debe identificar primero cada una de las necesidades de la seguridad, e implementar, desarrollar políticas, deberes y derechos, responsabilidades en la entidad, recursos informáticos en la organización, ante cualquier eventualidad que no se viole las políticas lo que cualquier evento que resulte en violación de la política se considera un incidente de seguridad.

1.8. Política de seguridad

Se regirán para controlar proporcionar, y gestionar la seguridad de la información, cuando se delimitan las políticas, según lo que el negocio necesita la organización; considerar los siguientes tres niveles de aplicación:

- Tecnologías
- Procesos
- Personas

La tecnología garantiza los ajustes técnicos necesarios para el tratamiento adecuado de los riesgos

1.8.1. La gestión del riesgo

1.8.1.1. Análisis y evaluación de riesgos

Para realizar el análisis y evaluación de los riesgos en las organizaciones es esencial Identificar, calificar y cuantificar. Se priorizan los riesgos de seguridad de la información (ver figura 2).

Figura 2. Resultado de análisis de gestión de riesgos
Fuente: Guía de implementación de ISO 27001

Es esencial para:

- Gestión del riesgo.
- Proposición de medidas de seguridad apropiadas. Consideraciones:
- Deben ser sistemáticas.
- Deben utilizar métodos concretos.

Se deben realizar periódicamente aspectos de análisis y evaluación de riesgos que deben ser contemplados son, deben ser llevados a cabo de manera sistemática con el fin de identificarlos analizando y evaluando el riesgo, el análisis de riesgo mide las amenazas y las vulnerabilidades

En los Impactos y actividades en un ambiente de trabajo serán con el fin de implementar con la adopción de las medidas del negocio y los requisitos de seguridad de la organización.

- Con los métodos específicos para permitir la comparación entre los resultados obtenidos y su reproducción.
- Debe realizarse periódicamente o cuando los requisitos de seguridad, activos, vulnerabilidades y/o los objetivos de negocio sufren algún cambio.

1.8.1.2. Elementos o Fases para la Implementación de un SGSI

La norma internacional de sistema de gestión (ver figura 3) de seguridad de la información ISO 27001 se resume en las siguientes fases a continuación se detalla:

Figura 3. Sistema de Gestión de Seguridad de la Información ISO 27001
Fuente: Guía de implementación de ISO 27001

1.8.1. Implantando la Norma ISO 27001

Para poder implementar un sistema de gestión de la información con la norma ISO 27001, se desarrolla uno de los ejes el cual es Evaluación de Riesgos**.** Este tipo de evaluación dentro de la implementación de la norma, permitirá a la empresa sea esta pública o privada, que se defina el alcance, aplicación de la norma, políticas, medidas a implantar, integrando este sistema para darle una mejoría continua a corto y largo plazo, en las normas ISO.

Para poder elegir una metodología correcta en la evaluación de riesgo para una empresa cualquiera que esta sea se debe tener como requisitos estandarizados y evaluación de riesgos. Consiste en las fases de la metodología ISO 27001 (ver figura 4).

Figura 4. Método de Evaluación y Tratamiento del Riesgo
Fuente: Guía de implementación de ISO 27001

1.- Identificar los Activos de Información y sus responsables (un activo todo aquello que tiene valor para la organización)

2.- Identificar las Vulnerabilidades de cada activo: aquellas que puedan sufrir daños sean estos estos físicos o ataques.

3.- Identificar las amenazas**:** toda aquella que pueda dañar o vulnerar información; así como desastres naturales, incendios o ataques de virus, espionaje etc.

4.- Identificar los requisitos legales y contractuales que la institución debe cumplir con sus clientes, socios.

5.- Identificar los riesgos: cuando se define qué tipo de amenaza, vulnerabilidad de cada activo que cause un daño total o parcial al activo de la información, en relación a la disponibilidad, confidencialidad e integridad del mismo.

6.- Cálculo del riesgo: Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.

7.- Plan de tratamiento del riesgo: implementado la norma ISO 27001 estará la organización preparada para definir sus políticas, asumir los tipos de riesgos por los activos, y realizar la definición de los mismos que serán los siguientes:

- Asumir el riesgo
- Reducir el riesgo
- Eliminar el riesgo
- Transferir el riesgo

La gestión de riesgos es parte esencial en cuanto a la prevención de fraude electrónico en línea, como es el, robo de identidad, daños de las páginas Web, la pérdida de los datos personales entre otras que son parte de la seguridad de la información. Si la organización no implementa una gestión de riesgos sólida, se exponen a los varios tipos de amenazas informáticas.

Según la norma internacional ISO / IEC 27001 seguridad de la información, es aquella que podrá ayudar a las diversas organizaciones y mejorar la gestión de sus riesgos de seguridad de la información.

1.8.2. Métodos en el tema de seguridad de la información

Actualmente existen otros estándares, tanto ISO/IEC como No ISO (ver tabla 3), además de metodologías relacionadas con el tema seguridad de la información, manejo de riesgos y campos similares.

Se analizarán a parte de los otros modelos de sistemas de información; entre las evoluciones estándares que estarán relacionados y que tendrán igualdades y diferencias de la seguridad de la información con sus diversas conceptuaciones y certificación de ellas. Los estándares seleccionados: ISO/IEC 13335, ISO/IEC 20000 y la norma AC SI 33 (norma no ISO, certificable).

Tabla 3. *Estándares de Evaluación de Riesgo*

Norma	ISO/IEC 27001	ISO		NO ISO
		ISO/IEC 13335	ISO/IEC 20000	ACSI33
Descripción Original	Tecnologías de la Información Técnicas de Seguridad Administración de Técnicas de Seguridad para la Información – Requerimientos	Administración de Seguridad de Tecnologías de la Información	Administra los Servicios de Tecnologías de la Información	Manual de Seguridad para Tecnologías de la Información y comunicaciones del Gobierno
Certificable	SI	NO	SI	SI
Ámbito o campo de acción	Engloba todas las áreas donde se puedan presentar incidentes en cuanto a seguridad de la información	Modelo de gobernabilidad de seguridad de la información bajo la gobernabilidad de Tecnología de la Información de acuerdo a la tecnología de la información	Está directamente relacionado a los servicios de tecnología son imprescindibles o fuertemente relacionados con el giro del negocio. Ej. Salud, entidades financieras, entidades públicas, etc.	Área de Tecnologías de la información, con obligatoriedad dentro del gobierno australiano
Ámbito de Recursos Humanos	Responsabilidad por las diferentes áreas en relación al información para evitar o gestionar incidentes en seguridad de la información	Experto en seguridad debe conocer varios campos como comunicaciones, base de datos, etc.	Se definen responsables para las distintas áreas relacionadas con el manejo o consumo de la información	Conceptualiza a través de SOP (Security Standard OperatingProcedures) a nivel de instrucciones a distintos niveles de uso o de la información.
Gestión con Terceras Partes	Riesgos relacionados con el intercambio de la información	Salvaguardas, que son obsoletas tras la publicación de ISO/IEC 27005:2008 y la norma ISO/IEC 18028-1,434722	Terceras partes o proveedores deberán integrar la cadena de servicios	Los proveedores deben estar involucrados como parte de proyectos, con los propietarios, usuarios.
Continuidad del servicio	Marco de gestión de continuidad, se incluyen los planes de contingencia	Evaluación general de los riesgos y vulnerabilidades de los sistemas, servicios y procesos de TI	A nivel de Planes de contingencia	Enfocado a las áreas de Infraestructura y Comunicaciones, mediante un SSP (System Security Plan)
Análisis de Riesgos	Identificación de riesgos asociados a la seguridad de la información de forma genérica.	Identificación, análisis y evaluación de riesgos de forma detalladas en varios capítulos, con explicación y ejemplos.	Riesgos asociados a la prestación de servicios de TI	Define y estructura un plan de gestión de riesgos para servicios de TI en entidades Gubernamentales australianas, estableciendo el contexto, diagnóstico, causas y consecuencias de los riegos
Gestión de Incidentes	Metodología para gestión de incidentes	Se ofrece lineamientos, no soluciones, para gestionar incidentes de seguridad y presentar las salvaguardas apropiadas para cada caso.	Metodología para gestión de incidentes	Responsabilidades mediante SOP (Security Standard OperatingProcedures) a nivel de planes de reconocimiento, auditoría de incidentes y responsables de procesos

Fuente: Elaboración propia

Tabla 4. *Tabla de Declaración de niveles de Riesgo*

RIESGO	DECLARACIÓN DE RIESGO		Probabilidad (%)	Impacto	Valor (%)	NIVEL DE VULNERABILIDAD
	CONDICIÓN	CONSECUENCIA				
Interrupciones en comunicaciones	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país	3	10	30	IMPORTANTE
Topología de red incorrecta	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional	3	20	60	INACEPTABLE
Mal dimensionamiento de las necesidades institucionales	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	Servicio lento y deficiente. Poco control sobre las actividades que se realizan en esos puntos. Se asocia a un mal servicio en general de toda la institución	3	10	30	IMPORTANTE
Capacitación del personal	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión	2	10	20	MODERADO
Disponibilidad de Recurso humano	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional	3	10	40	IMPORTANTE
Áreas Físicas para Data Center	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	Interrupción del servicio y daño físico en el equipamiento de servidores y equipos de comunicación.	1	20	20	MODERADO
Conexión a internet	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	Los sistemas misionales de la FGE se encuentran desarrollados para que sean accedidos por internet, por lo que al disponer de un servicio itinerante dificulta el ofrecimiento de servicios a los usuarios	3	20	60	INACEPTABLE
Central Telefónica	Equipamiento, infraestructura y recursos insuficientes	La comunicación telefónica es inexistente en algunos lugares, los servicios no son centralizados, dificultando las los funcionarios en puntos remotos del país.	1	10	10	TOLERABLE

Fuente: Elaboración propia

Tabla 5. Declaración de Vulnerabilidades

RIESGO	DECLARACIÓN DE RIESGO		Probabilidad (%)	Impacto	Valor (%)	NIVEL DE VULNERABILIDAD
	CONDICIÓN	CONSECUENCIA				
Equipos de cómputo para usuarios internos	Equipamiento obsoleto o inexistente en los puntos de atención	Descontento por la inequidad en la atención de los requerimientos de los usuarios internos. Lentitud en los procesos de atención al usuario. Manejo discrecional de los procesos oficiales para atención al público y fiscalía especializada.	2	20	40	IMPORTANTE
Equipamiento de servidores para uso institucional	Equipamiento insuficiente y de distintas generaciones	Sistemas no funcionan de manera óptima, con bajo nivel de procesamiento, sumado a un creciente número de instituciones que consumen, información de la FGE en decremento del nivel de satisfacción sobre el uso de las herramientas informáticas para los usuarios internos y externos,	3	20	60	INACEPTABLE
HelpDesk	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	Falta de retroalimentación para procedimientos de mejora. Discrecionalidad o inatención a las demandas del usuario. Retraso en la atención del usuario externo. Falta de métricas de rendimiento por analista, a cargo de las distintas áreas de soporte al usuario.	3	10	30	IMPORTANTE
Información de usuarios internos	Información para el control y monitoreo de actividades del usuario imprecisa	Perfiles y acceso de usuario inadecuados para recursos sensibles. Información desactualizada e incompleta	3	5	15	MODERADO
Catálogo de equipos	Catálogo de equipos manejado manualmente	Información imprecisa y desactualizada de catálogos es remitida periódicamente por los analistas provinciales en hojas electrónicas para que sea condensada en Quito	2	10	20	MODERADO

Fuente: Elaboración propia

Según el proceso que lleva la Fiscalía, parte desde que el usuario inicia su denuncia en la FGE, esta realiza un conjunto de procesos de Atención al Público, como lo son: Exámenes Médicos, Asesoría en la tipificación del Delito, Actividades Administrativas, entre otros, que se realizan en el Sistema Informático, de allí se desprende y procesa, almacena varias variables (hasta 50 variables) en el documento de la Denuncia de Delito de Acción Pública

La combinación de los datos reservados y públicos, como ejemplo tenemos que el conjunto de denuncias ingresadas; según los indicadores para los procesos gobernantes o que agregan de valor. Según estos indicadores de gestionan los derivados de los procesos que se necesitan en la cadena de valor de la institución, que se muestra de la siguiente forma (ver figura 5 y tabla 5).

Figura 5. Flujo proceso de gestión actual FGE
Fuente: Elaboración propia

Tabla 6. *Indicadores de proceso de gestión*

Proceso Estratégico	Indicador	Aplicación del indicador
Proceso Estratégico	-Número de proyectos para implementación de acuerdo al incremento o decremento de delitos en las provincias de la Costa.	- Mejorar, ampliar o agregar nueva infraestructura para mejorar el acceso de la ciudadanía a la investigación de los delitos.
	-proceso de ejecución de cada proceso.	- Mejorar el tiempo de ejecución de cada proceso
Proceso de Política Criminal	Cantidad de robo a personas desde las 00H00 hasta las 05H00 los días viernes- sábado	Coordinación con Policía Nacional o Policía Judicial se realiza operativos en los lugares y horas para su reclusión
Proceso en ámbito Procesal	Número de denuncias por Especialidad	Evaluación de carga laboral para reforzamiento mediante directrices o reestructuración de Especialidades
Proceso de Calidad	Número de ingresos equivocados por parte de los asesores	Mejoras en el procedimiento para evitar futuros errores

Fuente: Elaboración propia

Tabla 7. *Tipificación del Delito*

FORMA DEL DELITO	PROVEEDORES	ENTRADAS
FLAGRANTES	POLICIA NACIONAL, POLICIA DE TRANSITO y POLICIA JUDICIAL	✓ PERITAJES DE ATENCIÓN ✓ PERITAJES DE TRANSITO ✓ FLAGRANTES
NO FLAGRANTES	CIUDADANIA, ABOGADOS, DINAPEN, POLICIA NACIONAL, MEDIOS DE INFORMACIÓN, CONTRALORIA, INSTITUCIONES DEL ESTADO	✓ DENUNCIAS ORALES ✓ DENUNCIAS ESCRITAS ✓ ACTAS DE LEVANTAMIENTO DE CADAVER ✓ PARTES POLICIALES ✓ INFORME DE CONTRALORIA ✓ INFORME PARA INVEST. DE OFICIO
ACTOS ADMINISTRATIVOS	CIUDADANIA	✓ SOLICITUDES DE SERVICIOS

Fuente: Elaboración propia

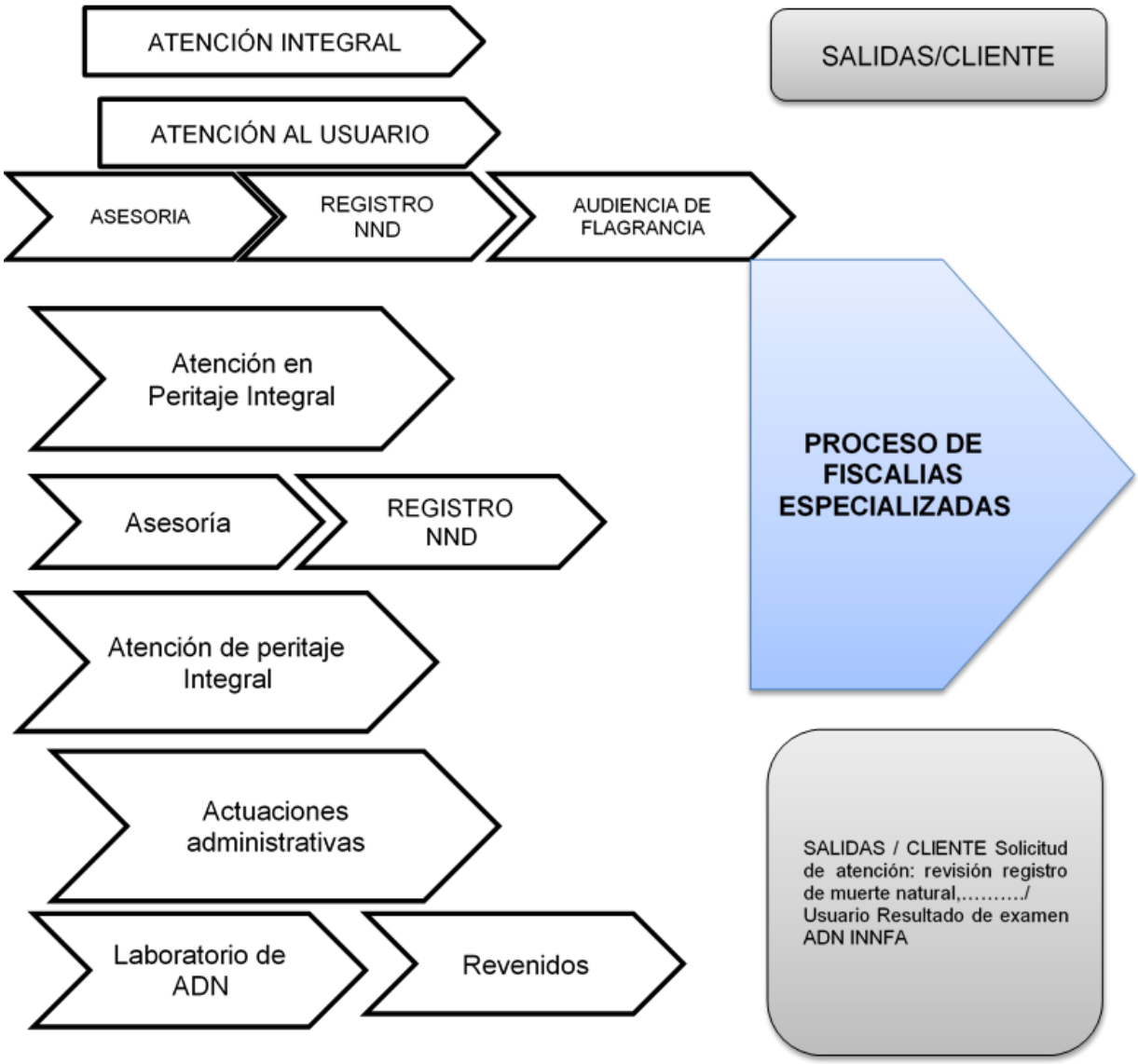


Figura 6. Esquema de procesos de la FGE
Fuente: Elaboración propia

1.8.3. Clasificación del Riesgo

Se pueden clasificar los riesgos de las siguientes maneras:

- **Riesgos estratégicos:** Los objetivos estratégicos deberán estar orientados en conjunto con la misión y visión de la institución para la cual se realiza este tipo de monitoreo de los riesgos.
- **Riesgos Operativos:** Se relaciona con el área operativa de la empresa en el cual se observa la deficiencia de los sistemas de información aplicados en la entidad , y que su información deberá

ser descentralizada, e ineficiente, falta de compromiso con los objetivos que se ha trazado la institución.

- **Riesgos Financieros:** Los recursos de la entidad esto la planificación, ejecución presupuestaria donde se incluyan el estado financiero, bienes con un manejo claro, transparente dependerá el éxito en la ejecución de los proyectos emprendidos proyectos.

- **Riesgos de cumplimiento:** Relacionados con el cumplimiento de requisitos legales, contractuales, éticos y el compromiso con las áreas a las que se debe, generalmente al público en general.

- **Riesgos de Tecnología:** Capacidad que tiene la organización para poner a disponibilidad sus elementos tecnológicos para satisfacer las necesidades inmediatas, futuras dentro de un plazo máximo previsto para para cumplimiento a los objetivos de la organización**.**

1.8.4. Metodologías para la Evaluación de las Vulnerabilidades

Mediante la metodología ISO para análisis y evaluación de vulnerabilidad, de la situación que esté pasando la organización en las siguientes etapas:

- Identificación
- Medición
- Control
- Monitoreo.

1.8.5. Identificación de Vulnerabilidad

Según la organización cualquiera sea esta, pública o privada, e independientemente de su tamaño; la vulnerabilidad a recibir este tipo de ataques es igualmente permanente, de correr peligro, que afectara la supervivencia o éxito en determinadas áreas.

En la misma línea, podemos observar que no es posible eliminar completamente las vulnerabilidades, pero es posible gestionarlo determinar niveles aceptables para cada organización.

Un ejemplo de cómo determinar niveles aceptables de vulnerabilidad en una organización una vez que se han determinado las posibles vulnerabilidades, de acuerdo a los indicadores de cada empresa o institución en el caso de la fiscalía general se lo detalla a continuación con un nivel de escala probabilidad, impacto, valor que se genera el nivel de vulnerabilidad que se encontraría.

Tabla 8. *Declaración de las Vulnerabilidades*

Vulnerabilidad	DECLARACIÓN DE VULNERABILIDAD		Probabilidad (%)	Impacto	Valor (%)	NIVEL DE VULNERABILIDAD
	CONDICIÓN	CONSECUENCIA				
Interrupciones en comunicaciones	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país	3	10	30	MODERADO
Topología de red incorrecta	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional	3	20	60	INACEPTABLE
Mal dimensionamiento de las necesidades institucionales	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	Servicio lento y deficiente.	3	10	30	MODERADO
		Poco control sobre las actividades que se realizan en esos puntos	3	10	30	MODERADO
		Se asocia a un mal servicio en general de toda la institución	3	10	30	MODERADO
Capacitación del personal	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión	2	10	20	MODERADO
Disponibilidad de Recurso humano	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional	3	10	40	IMPORTANTE
Áreas Físicas para Data Center	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	Interrupción del servicio y daño físico en el equipamiento de servidores y equipos de comunicación.	1	20	20	MODERADO

Fuente: Elaboración propia

1.8.6. Procedimiento de control para gestionar los riesgos:

Como parte de los procedimientos de control es necesario contar con actividades de monitoreo y revisión para:

- Detectar errores que pueden ser producidos por el procesamiento de información
- Identificar problemas o brechas de seguridad
- Los directivos determinaran y evaluaran, las actividades realizadas, los resultados obtenidos han garantizado seguridad en la información, a nivel de personal, procedimientos o dispositivos tecnológicos.
- Los indicadores previamente establecidos, ayudaran a establecer, detectar y prevenir eventos e incidentes de seguridad.
- Determinar si las acciones correctivas utilizadas en un incidente resolvieron el problema con efectividad.

Además, la revisión de las tareas de forma periódica, con mediciones de eficacia y eficiencia del SGSI, vigilando con rigurosidad si continua con las políticas y objetivos por los que fue implementados, organizando y evaluando los resultados de las auditorias de seguridad que se han aplicado, tipos de incidentes reportados, sugerencias y observaciones de todos los actores implicados.

Establecer mediciones para la efectividad de cada uno de los controles implementados, con vigilancia que cumplan completamente los objetivos que se especificaron, evaluar lo siguiente:

- Riesgos previstos
- Riesgos residuales
- Niveles de aceptación de Riesgo

Todos estos tienen que estar enfocados en los cambios que se pueden presentar en la Tecnología, objetivos y procesos institucionales, Amenazas

identificadas, Efectividad de los controles implementados, Eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

Realizar una permanente revisión del SGSI por parte de los directivos para determinar si los alcances planteados originalmente siguen siendo los más adecuados y que las mejoras que se implementan son efectivas y evidentes.

Además, las actividades de control, también abarcan la permanente actualización de los planes de seguridad en función de las observaciones, conclusiones o nuevos hallazgos encontrados durante las actividades de monitorización y revisión de los procesos y el mismo SGSI.

1.8.9. Act: Mantener y mejorar el SGSI

Se deben implantar en el SGSI las mejoras identificadas.

Realizar las acciones preventivas y correctivas adecuadas, y coordinar eventos para compartir las lecciones aprendidas de las experiencias propias y de otras organizaciones.

Establecer niveles de profundidad en las explicaciones o comunicaciones entre los interesados de acuerdo al detalle que se necesita cada parte para continuar con el proceso normal de sus actividades. Verificar que las mejoras introducidas alcanzan los objetivos estratégicos.

La adopción de un SGSI debe ser una decisión estratégica para una organización, en este caso la Fiscalía General del Estado. Se considera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple. Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

La información, conjuntamente con los procesos y sistemas relacionados para el uso de ella, son activos muy valiosos de cualquier institución, el poder disponer de los elementos de la seguridad informática (confidencialidad, integridad y disponibilidad) constituye una parte esencial para mejorar o mantener los niveles de calidad.

Según investigación de campo realizada en un 50% de las instituciones financieras en el Ecuador utilizan el Modelo ISO 27001, en un promedio las instituciones financieras invierten en un 43%, las cooperativas de ahorro y crédito en 37%; utilizan cualquier otro modelo con políticas poco confiables, tomando como referencias diferentes fuentes bibliográficas donde se reflejan cifras aproximadas de inversión de las diferentes entidades del sistema financiero del país y que con una recolección de datos cualitativo, materiales digitales audiovisuales, entre otras fuentes de estudio se han podido verificar su veracidad y que serán analizadas (Sánchez, 2013).

Una vez que se haya aplicado el Sistema de información con la norma ISO 27001 la estructura para mejorar de manera continua, paulatina a la Fiscalía General del Estado si se cumple con los objetivos estratégico que estarán de la mano con la misión visión de la Fiscalía que es el brindar una información ágil y oportuna , contribuyendo con el medio ambiente, los principios de celeridad procesal y economía procesal daría como resultado que los procesos automatizados, sin tener la mayor cantidad de documentos en físico que hasta ahora la fiscalía maneja para resolver un causa en cualquier tipo de delito como hemos podido observar los procesos que se llevan hoy en día en la FGE, se encuentra entramados de procesos documentales engorrosos desde el ingreso de la documentación hasta que termina su papel la FGE.

1.9. Aplicando ISO 27001 FGE

1.-Atención al Usuario --- Debe de ser en Línea

2.-Atención Integral --- En línea

Ingreso de la denuncia ---- en línea no solo la de documentos extraviados si no todas aquellas ciudadanas que requieran una ágil atención.

3.- Documentación digitalizada con la misma validez, que la documentación física.

4.- En el caso de victimas de ciberacoso, defraudación, fraude electrónico si se realiza audiencia de flagrancia a la denuncia o formulación de cargo en línea por el principio de celeridad procesal.

5.- Resultados de las investigaciones deben de ser reflejados en sistema con un minucioso detenimiento para que el usuario no tengas dudas de la transparencia.

6.- De ser el caso que haya un ingreso erróneo por parte del digitador, sorteo, tipicidad del delito deberá ser inmediatamente resuelto para descongestionar el número de delitos presentados dentro de la semana como parte de los indicadores de gestión de la ISO, evitando así el 7.- congestionamiento.

7.- Cada uno de los procesos deberá ser revisado y monitoreado por la institución para que se cumpla con los plazos establecidos que es un factor importante para la economía procesal de cada institución, y cada entidad si no se cumplen con los procesos, involucrados se dirijan a enfocarse y evitar que haya retrasos en la entrega, posterior al usuario.

Si no se cuenta con una tecnología adecuada para que la FGE, pueda realizar la automatización de los procesos internos que permiten que realice toma de decisiones dentro de la misma que no permita lo siguiente:

- Fuga de la información clasificada como reservada
- Adulteración de los resultados de laboratorios que son ingresados a una base datos, como pruebas de ADN, pruebas dactilares, pruebas periciales que dentro de ellas se encuentran las realizadas a equipos

tecnológicos de respaldo, cada una de estas pruebas mencionadas tienen como objetivo el mostrar la culpabilidad de un individuo.

- Tiempo que concluye cada proceso para mejorar la relación entre la fiscalía y el usuario quien es el encargado de creer en un sistema obsoleto o modernizado que dé resultados en el menor tiempo posible,
- De los resultado obtenidos el fiscal podrá tomar decisiones adecuadas para resolver todas las actuaciones a realizar es porque cada indicador mostrara el riesgo que se corre tanto con la infraestructura, tecnología, tiempos de procesos que son perjudiciales en un proceso penal.

CAPÍTULO II. MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de la investigación

La investigación realizada busca tener indicadores que permitan medir los riesgos en una menor cantidad de tiempo en la Fiscalía y que esta al implementar el modelo ISO 27001 agilice significativamente se gestión. Los riesgos y vulnerabilidades afectan a la ciudadanía, entidades públicas y privadas y al estado en general.

Este tipo de modelo tendrá el éxito necesario si se aplica de manera eficiente al determinar los riesgos de la entidad jurídica al momento de detectarse una amenaza y poder tener una mejor adecuación del hecho ilícito en tiempo, espacio, lugar.

Para determinar los datos se realizó una investigación:

- Descriptiva
- Método NO experimental

2.2. Tipo de investigación

Es una investigación cualitativa, el nivel de la investigación es descriptivo, no experimental y transversal. Este tipo de método de investigación nos ayudará a realizar la verificación de los datos de manera cualitativa de una manera exploratoria y se dará en base a la credibilidad, la confiabilidad, la transferibilidad y la consistencia general.

Los investigadores tienden a colectar datos en el sitio donde los participantes experimentan el problema o la situación bajo estudio.

2.2.1. El método No experimental.

En el método de desarrollo para investigación de este proyecto es verificar los rasgos y características de la situación en este caso cuales son las características que definen las demoras:

Pueden ser la base de otros tipos de investigación más compleja.

- No plantean hipótesis
- Se basan en encuestas, entrevistas, observación y revisión documental.
- Sobre qué o sobre quiénes se recolectarán los datos (personas, grupos, comunidades, objetos, animales, hechos) (Huescas, 2011)
- Estudios exploratorios
- Estudios descriptivos

2.3. Procedimientos de colección de datos cualitativos

- **Observación cualitativa**: El investigador toma nota en el campo de trabajo según el comportamiento del sitio donde obtuvo el problema
- **Documentos cualitativos**: Entre estos documentos tenemos documentos públicos (periódicos, minutas de reuniones, reportes oficiales) o documentos privados (diarios personales, cartas, correos electrónicos).
- **Materiales digitales y audiovisuales**: Los materiales pueden ser textos, fotografías, correos electrónicos, textos de social media.

2.4. Operacionalización de las Variables de la investigación.

Para Nivel Descriptivo

Variable principal: De Interés:

- **Seguridad informática:** Gestión de procesos de riesgo cibernético en el sector financiero

Variables segundarias: De Caracterización.

- **Evaluación de riesgos (VI.1)-**sistemas de gestión define el riesgo como el efecto que genera la incertidumbre, puede ser positivo o negativo, debido a la falta de información de la situación, proceso o procedimiento
- **Tratamiento del riesgo (VI.2)-**Medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI
- **Funcionabilidad del SGSI (VI.3)-**Hacer una pausa y definir procesos y procedimientos como consecuencia, de lo que se debe de hacer, cuando, hacerlo
- **Control procedimental obligatorio (VI.4)-** gestionar la seguridad de la información en organismos y empresas independientemente de su tamaño, objetivos o estructura,

2.5. Fuentes y técnicas e instrumentos para la recolección de información

2.5.1. Fuentes de información

Al ser una investigación tipo documental se utilizó fuentes primaria y secundaria de organismos gubernamentales y no gubernamentales afines a la información.

Fuentes primarias: Se identificó la información procedente de:

- Revisión de informes emitidos por el INEC desde el 2014 al 2020.
- Información de la Superintendencia Bancos y Seguros.
- Datos Fiscalía General del Estado.
- Modelos de seguridad

Fuentes secundarias:

- Información estadística y documental de otras fuentes de información.
- Información de artículos científicos y revistas oficiales.
- Página web del Instituto Nacional de Estándares y Tecnología (NIST), informes de estándares ISO.
- Publicaciones de tesis de investigación científica.
- Revisión literaria sobre el tema.

2.5.2. Técnicas para la recolección de información.

Técnica de investigación estadística.

En este tipo de técnica se usa para extraer los datos estadísticos que se encuentran base de datos públicos de diferentes organismos gubernamentales y no gubernamentales involucrados con la información; para levantar información.

2.6. Técnica de investigación documental.

Las fuentes sustentadas son: tesis, revistas, páginas web, libros, informes técnicos, artículos científicos y toda aquella fuente válida, de las variables garantía, gobernanza, identidad y control de acceso, gestión de riesgos, servicio, despliegue, cumplimiento.

Escala aplicada para la evaluación de las variables: Se adecua a que se puede realizar para investigar un fenómeno de la investigación, y que se puede medir fenómenos con métodos positivos, hechos sociales, comportamientos, individuales en el caso de esta investigación, es el hecho de mejorar los tiempos de la resolución de una denuncia, este tipo de método permitirá realizar un método más fiable o factible. Dando respuestas más favorables, seguras que muestren la opinión objetiva, precisa. La escala de asignación empleada para medición del riesgo se expone en la tabla 8.

Tabla 9*. Escala de Likert para la medición de los riesgos informáticos*

ESCALA	CRITERIO	RANGO	
5	En total acuerdo con la seguridad	81%	100%
4	En acuerdo con la seguridad	61%	80%
3	Ni en acuerdo ni en desacuerdo con la seguridad	41%	60%
2	En desacuerdo con la seguridad	21%	40%
1	En total desacuerdo con la seguridad	0%	20%

Fuente: Elaboración propia

2.6.1. Tratamiento de la información

Para la resolución y tratamiento de la información se realizó con el SPSS, para calcular numéricamente y establecer comparaciones, tendencias de pérdidas y ganancias tanto de la banca, o el sistema financiero como de los usuarios en tiempo, la economía, un análisis de tabla de distribución de frecuencias, descriptivos, análisis de varianza y tabla de contingencia (tabla cruzada), gráficos de sectores, barras e histograma.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual.

3.1.1. Análisis de la Fiscalía en el sector de los delitos informáticos sin el Modelo ISO 27001.

De acuerdo a la investigación realizada la FGE no tiene el equipo técnico suficiente para poder resolver en el menor tiempo posible las denuncias presentadas por un acceso no consentido de la información, no se encuentra orientada a dar una solución rápida y efectiva al usuario quien a la final es el perjudicado.

En este desarrollo se evidencio que desde años atrás se vienen realizando este tipo de delitos informáticos que en el COIP se denomina delitos por medios electrónicos no dándoseles el nombre adecuado que por ejemplo robo de dinero o en el caso de fraude que son los nombres comunes que hemos visto dentro de la investigación.

Para cada caso hay una situación totalmente distinta para tratar la información a pesar de que la evidencia entren a una cadena de custodia no es factible por ejemplo tener que llevarse un CPU, una memoria, cuando la información proporcionada debe de ser directamente dada por la institución financiera a la cual el usuario le ha dado la confianza de invertir su dinero.

Si tan solo cada usuario pudiera analizar cada centavo que se desvía de cuenta cada vez que realiza una transacción en línea vería que no es difícil que, como en otras investigaciones se determina que quienes están involucrados y en muchas ocasiones son los mismos empleados, pero como el personal que realiza el peritaje no es lo suficientemente calificado no se da cuenta de este tipo de anomalías.

Para ellos veremos un análisis de las pérdidas de las instituciones bancarias versus el análisis de que analizan si se sugiere un nuevo modelo que permita reducir primero la economía procesal que es el tiempo que requiere la fiscalía

para poder determinar culpables, la sanción a determinar según nuestra legislación.

De la misma manera, se ha obtenido información de las mismas instituciones reguladoras sobre la ejecución en relación a inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques. Se adjunta Tabla 9

3.1.2. Análisis comparativo, evolución, tendencias y perspectivas

Tabla 10. *Inversión en infraestructura y sistemas tecnológicos*

INVERSION EN INFRAESTRUCUTURA Y SISTEMAS TÉCNOLOGICOS PARA FRENAR LOS CYBERATAQUES				
	AÑO 2017	**AÑO 2018**	**AÑO 2019**	**AÑO 2020**
		BANCOS		
DATA CENTER FISICO	$20.700,00	$137.895,00	$117.987,00	$121.554,00
DATA CENTER VIRTUAL	$2.345,24	$2.550,25	$2.100,35	$3.713,44
		COOPERATIVAS		
DATA CENTER FISICO	$15.700,00	$21.547,00	$33.050,00	$47.658,00
DATA CENTER VIRTUAL	$1.525,25	$1.736,14	$1.812,23	$1.800,20
Total de Inversiones	**$40.270,49**	**$163.728,39**	**$154.949,58**	**$174.725,64**

Fuente: Icen 2020

Tabla 11. Comparación de pérdidas e inversión

AÑO	TOTAL PERDIDAS ALCANZADAS POR LAS INSTITUCIONES FINANCIERAS Y COOPERATIVAS DE AHORRO (Y)	TOTAL INVERSION EN INFRAESTRUCTURA Y SISTEMAS TÉCNOLOGICOS PARA FRENAR LOS CYBERATAQUES (X)	Relacion Inversion contra Perdidas
2017	$445.167,00	$40.270,49	0,09
2018	$372.791,00	$163.728,39	0,44
2019	$333.379,00	$154.949,58	0,46
2020	$285.143,00	$174.725,64	0,61

Fuente: Icen 2020

Ambas tablas permitirán establecer si existe relación directa entre las pérdidas de las instituciones financieras por ataques informáticos frente a la inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques por parte de las mismas. El parámetro del tiempo para este estudio se considera desde el año 2017 hasta 2020.

3.1.3. Resultados estadísticos de las variables analizadas.

Mediante la determinación de análisis en caso de existir o no una relación directa entre las variables dependiente “total perdidas alcanzadas por las instituciones financieras y cooperativas de ahorro” (Y) y la variable independiente “total inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques” (X).

Entonces, se podría establecer si existió una importancia. También, se empleará un modelo de regresión lineal simple para obtener un valor de correlación R^2. Se aplicó, el paquete estadístico SPSS. Mediante la obtención de una ecuación de la recta a partir de la nube de puntos planteada por las variables (Y), si es afectada por los cambios que se generen por el aumento de la variable (X) y como se van asociando en los periodos estudiados. La ecuación de la recta es:

$$Y = 4{,}86E5 - 0{,}95*X$$

El total, perdidas alcanzadas por las instituciones financieras y cooperativas de ahorro = 4,86E5 – 0,95*(Total inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques)

También, se puede evidenciar la reducción de las pérdidas de las instituciones financieras, causada por el incremento de las inversiones en ciberseguridad. La tendencia se puede ver mediante en estadístico R^2, y la tendencia de la relación (ver gráfico 3)

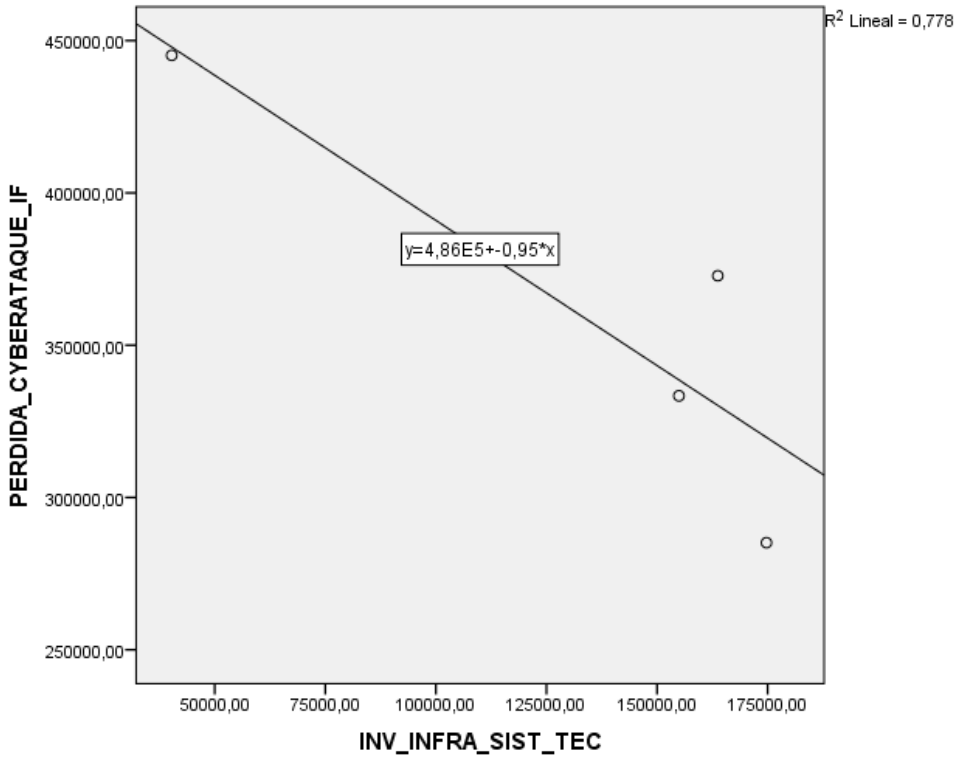


Gráfico 3. Determinación lineal y formula de tendencia de inversión contra perdidas
Fuente: Elaboración propia

La disminución de las perdidas, fue acusada de manera positiva por el incremento de la inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques.

Además, se evaluó el test de correlación, es media alta con -0.882 de asociación y su nivel de significancia es aceptable. Se puede apreciar en la Tabla 12 de Correlaciones. En pocas palabras, que la inversión en infraestructura y sistemas tecnológicos está relacionada con la disminución de pérdidas por ciberataques. Para la construcción del modelo de regresión lineal como variable independiente o, de entrada, se consideraría la inversión en infraestructura y sistemas tecnológicos (ver tabla 13).

Tabla 12. Correlación de Pérdidas

Correlaciones

		PERDIDA_CYBERATAQUE_IF	INV_INFRA_SIST_TEC
PERDIDA_CYBERATAQUE_IF	Correlación de Pearson	1	-,882
	Sig. (bilateral)		,118
	N	4	4
INV_INFRA_SIST_TEC	Correlación de Pearson	-,882	1
	Sig. (bilateral)	,118	
	N	4	4

Fuente: Elaboración propia

Tabla 13. Coeficientes Infraestructura

Coeficientes

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.
		B	Error estándar	Beta		
1	(Constante)	486251,999	51797,465		9,388	,011
	INV_INFRA_SIST_TEC	-,953	,360	-,882	-2,649	,118

a. Variable dependiente: PERDIDA_CYBERATAQUE_IF

Fuente: Elaboración propia

Tabla 14. Variable perdida Cyberataque

Variables entradas/eliminadas

Modelo	Variables introducidas	Variables eliminadas	Método
1	INV_INFRA_SIST_TEC[b]	.	Intro

a. Variable dependiente: PERDIDA_CYBERATAQUE_IF

b. Todas las variables solicitadas introducidas.

Fuente: Elaboración propia

Para el modelo de regresión probado con una variable independiente, se explica que el 77,8% de la varianza de la variable dependiente (R cuadrado: .778). Total, las pérdidas de las instituciones financieras por ataques informáticos puede explicarse por los predictores en este caso la variable inversión en infraestructura y sistemas tecnológicos (ver tabla 15).

Resumen del modelo.

Tabla 15*. Resumen de Modelo*

Resumen del modelo[b]

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Durbin-Watson
1	,882[a]	,778	,667	39010,67474	1,707

a. Predictores: (Constante), INV_INFRA_SIST_TEC

b. Variable dependiente: PERDIDA_CYBERATAQUE_IF

Fuente: Elaboración propia

En los resultados obtenidos, el estadístico de prueba dio una asociación de variables aceptable de 0.778. No obstante, ratifica el rechazo de la hipótesis nula que La total inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques no tuvo ninguna incidencia sobre la reducción de las pérdidas alcanzadas por las instituciones financieras y cooperativas de ahorro.

Por consiguiente, se acepta la H_1, que plantea que la inversión en infraestructura y sistemas tecnológicos para frenar los ciberataques, incide de manera positiva en las reducciones perdidas alcanzadas por las instituciones financieras y cooperativas de ahorro.

- Distribución de información general de la empresa.
- Integración de los sistemas de información de todos los procesos.
- Manejo seguro de transacciones electrónicas como transferencias bancarias, comercio electrónico, entre otras.
- Control de proveedores

3.2. Análisis comparativo, evolución, tendencias y perspectivas

Vulnerabilidad del sector financiero

El sector financiero es particularmente vulnerable a los ataques cibernéticos. Las instituciones financieras son blancos interesantes por su función vital en la intermediación de fondos. Un ataque cibernético exitoso contra una institución podría propagarse rápidamente a través del sistema financiero, ya que está

sumamente interconectado. Muchas instituciones siguen empleando sistemas más antiguos, que podrían no resistir a los ataques cibernéticos. Además, un ataque exitoso puede tener consecuencias sustanciales directas por las pérdidas financieras causadas, pero también costos indirectos, como el perjuicio a la reputación.

Algunos casos recientes de gran notoriedad han introducido progresivamente al riesgo cibernético en el orden del día del sector oficial, e incluso de los organismos internacionales. Pero el análisis cuantitativo de este riesgo aún está en sus labores, especialmente debido a la falta de datos sobre el costo de los ataques y las dificultades para modelarlo.

Un estudio reciente del FMI provee un marco para analizar las pérdidas que pueden resultar de los ataques cibernéticos, especialmente en el sector financiero.

3.2.1. Estimación de las posibles pérdidas

El marco del modelo usa técnicas obtenidas de las ciencias actuariales y la medición del riesgo operativo para estimar las pérdidas acumuladas como consecuencia de los ataques cibernéticos. Esto requiere evaluar la frecuencia de los ataques a las instituciones financieras y formarse una idea de la distribución de las pérdidas resultantes de estos incidentes. Luego se pueden utilizar simulaciones numéricas para estimar la distribución de las pérdidas acumuladas causadas.

Ilustramos nuestro marco empleando un conjunto de datos que incluyen las pérdidas recientes por ataques cibernéticos en 50 países. Así se ejemplifica una forma de estimar las posibles pérdidas de las instituciones financieras. Esta labor es compleja y se dificulta aún más debido a las importantes carencias de los datos sobre el riesgo cibernético. Además, afortunadamente, todavía no ha habido un ataque exitoso a gran escala contra el sistema financiero.

Por ende, nuestros resultados deben considerarse como un simple ejemplo. Si se toman en sentido literal, indican que el promedio de las posibles pérdidas

anuales resultantes de los ataques cibernéticos puede ser significativo y ubicarse en el orden del 9% de los ingresos netos de los bancos a nivel mundial, es decir, unos USD 100.000 millones. En un caso hipotético de gravedad, en que la frecuencia de los ataques cibernéticos fuera dos veces superior a la registrada hasta ahora y con un mayor contagio, las pérdidas podrían ser 2½–3½ veces mayores, o sea, ascender a un monto de entre USD 270.000 millones y USD 350.000 millones.

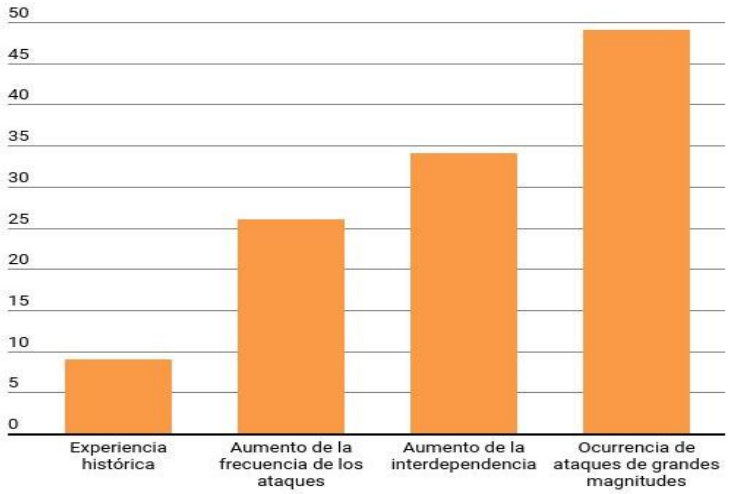


Gráfico 4. Experiencia histórica

Fuente: Elaboración propia

3.2.2. El camino a seguir

Hay un amplio margen para mejorar las evaluaciones de riesgo. La recopilación por parte de los gobiernos de datos más granulares, firmes y completos sobre la frecuencia y los efectos de los ataques cibernéticos ayudarían a evaluar el riesgo para el sector financiero.

Se prevé que los requisitos de declaración de filtraciones, como los considerados en el marco del Reglamento General de Protección de Datos de la UE, ayuden a tener un mayor conocimiento de los ciberataques. Se podría utilizar el análisis de casos hipotéticos para evaluar integralmente la forma de propagación de los ataques cibernéticos y para idear respuestas adecuadas de las instituciones privadas y los gobiernos.

También se debe profundizar la labor tendiente a entender cómo fortalecer la

resiliencia de las instituciones e infraestructuras financieras, tanto para reducir las posibilidades de éxito de un ataque cibernético como para facilitar una recuperación rápida y sin contratiempos. Además, en muchas partes del mundo, se debe fortalecer la capacidad del sector oficial de vigilar y regular estos riesgos.

En resumen, es necesario fortalecer los regímenes normativos y de supervisión para hacer frente al riesgo cibernético, y los esfuerzos deben centrarse en el establecimiento de prácticas de supervisión eficaces, pruebas de vulnerabilidad y recuperación, y planes de contingencia que sean realistas. El FMI está brindando asistencia técnica para ayudar a los países miembros a mejorar sus regímenes normativos y de supervisión.

Los bancos y seguros están inmersos en cambios radicales donde su entorno de negocios, cultural y tecnológico ha alterado la forma en la cual operan. Esta ola de cambios tiene una base importante en las tecnologías digitales, las cuales son adoptadas con el propósito de mejorar la experiencia de los clientes y mejorar los niveles de eficiencia de las organizaciones.

La realidad es que este cambio no es una opción para los bancos y seguros, sin embargo, los programas de adopción de estas tecnologías digitales no transparentan de forma integral cuáles son los riesgos a los que se exponen las organizaciones. Uno de los aspectos más importantes a considerar es la ciberseguridad**.**

Durante los últimos meses hemos sido testigos de una ola muy grande ciberataques en la región y Ecuador no es ajeno a este fenómeno. A pesar de esta situación, un estudio global de PwC sobre delitos económicos indica que los delitos informáticos ocupa el segundo lugar en los delitos económicos reportados.

El mismo estudio muestra que a 61% de los CEO les preocupa la ciberseguridad de sus empresas, sin embargo, solo 37% de ejecutivos indica que sus organizaciones tienen un plan de respuesta ante un delito informático. Las cifras son claras, los incidentes relacionados con ciberseguridad están

presentes y confirman ciertas tendencias: el origen de los incidentes de seguridad los realiza principalmente colaboradores y ex empleados; el principal objetivo de los ataques es el robo de correos corporativos, ataques a dispositivos móviles, etc.

Ante esta situación, las organizaciones se ven expuestas a estos riesgos y tienen la necesidad de dar respuesta mediante un esquema de protección apropiado. Este esquema debe tener la aprobación de la Alta Dirección, la cual necesita tener confianza sobre los programas de ciberseguridad de sus organizaciones con base en una adecuada evaluación de riesgos. El programa debe considerar: la preocupación sobre la ciberseguridad y privacidad, los cambios organizacionales, la presión regulatoria y la disrupción digital. Con esta evaluación se podrán establecer de forma eficiente y efectiva, las contramedidas que deben implementarse.

3.3. Presentación de resultados y discusión

En los resultados de la encuesta realizada a los fiscales a nivel provincial, se pudo desarrollar un levantamiento de información acerca del sistema nacional de investigación que realiza la Fiscalía para poder desarrollar mejoras en el proceso de encontrar a los culpables de alguna intromisión en los sistemas de las entidades financieras, en las cuales los más perjudicados son los usuarios quienes están dilatando el regreso de su dinero, ya que para pedir un video de vigilancia la fiscalía debe oficiar y la institución para dar ese video se demora alrededor de un mes dando como resultado que el usuario por lo regular para que se le devuelva su dinero o el monto perjudicado prácticamente se realiza alrededor de un año y un poco más, siendo el más perjudicado. Si se toma decisiones a tiempo será de ayuda FGE, como para el usuario quien es el que busca la ayuda del organismo estatal para que se repare integralmente el daño acontecido.

3.3.1. Análisis de la encuesta

En esta encuesta podemos observar que para ellos los celulares en un 26%, computadoras en un 35%, redes sociales25%, Links a través de la red en un

14% puesto que según los casos ingresados en las diferentes de asuntos rápidos, de los cuales vemos que han tenido mayor incidencia que los delitos informáticos se han dado por las computadoras, a través de las redes de computadoras que han sido fácilmente manipulables por los Delincuente informático (ver gráfico 5).

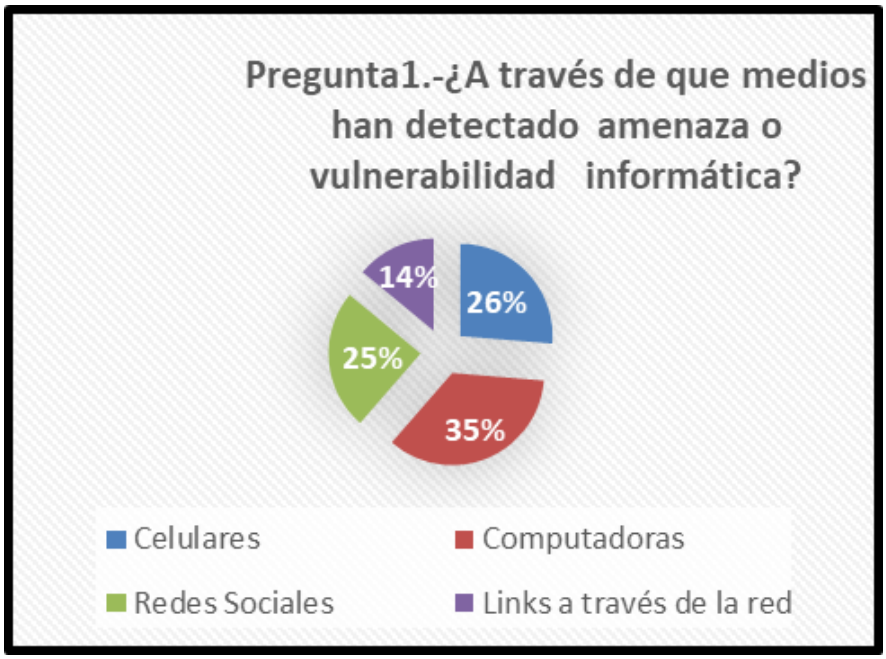


Gráfico 5. Pregunta 1
Fuente: Elaboración propia

En la segunda pregunta los resultados son los siguientes: Bancarias 47%, mutualista 15%, cooperativas de ahorro y crédito 26%, ninguna 12%; es por esto que según la pregunta No. 2 las entidades financieras en el Ecuador que han tenido mayores ataques han sido los banco quienes han sido vulnerados en sus sistemas informáticos tomando información privada de los usuarios (ver gráfico 6).

Gráfico 6. Pregunta 2
Fuente: Elaboración propia

La tercera pregunta se resume la información recabada tenemos que varias de las personas encuestadas el proceso llevado por la Fiscalía es demasiado lenta según el 52%, y en un 16% es oportuna, y en un 32% aseguran que es ágil con el proceso que lleva actualmente (ver gráfico 7).

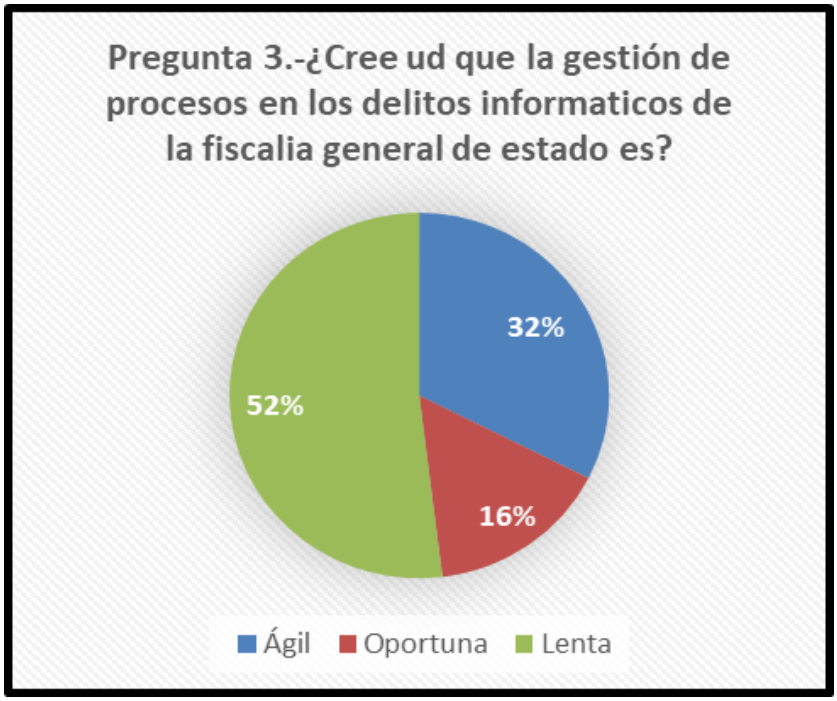


Gráfico 7. Pregunta 3
Fuente: Elaboración propia

Se evidencia según la encuesta que el tiempo que duraría investigación en Fiscalía **el** 88% 6 meses piensa que sería bueno para agilizar el proceso de investigación previa, y demás pericias, 12% 1 año, 0% 2 años para ellos si se lleva un buen sistema de un modelo ISO 27001 (ver gráfico 8).

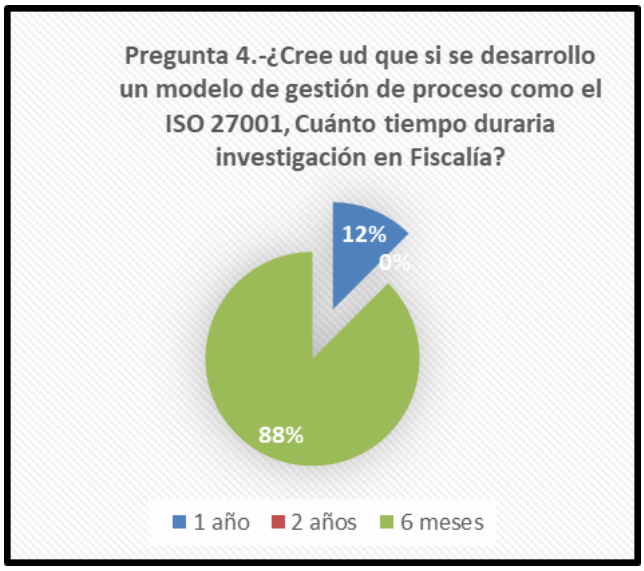


Gráfico 8. Pregunta 4
Fuente: Elaboración propia

En la pregunta cinco el 85% está de acuerdo con manejar el Plan de Riesgo en las entidades financieras para valorar culpabilidad y el 15 % no comparte igual opinión (ver gráfico 9).

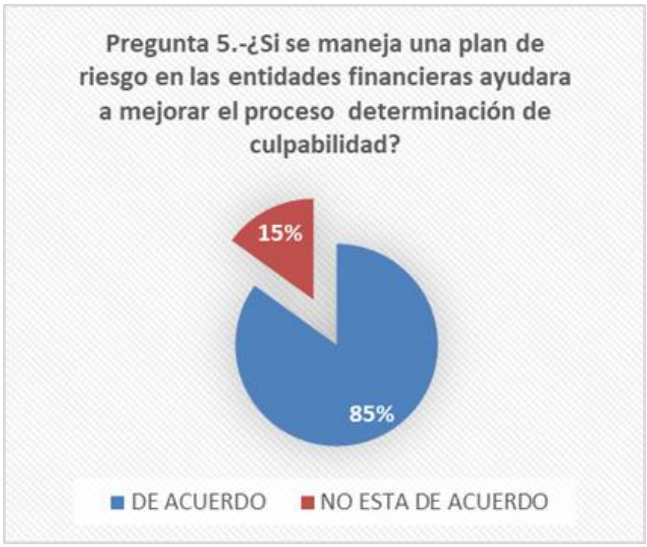


Gráfico 9. Pregunta 5
Fuente: Elaboración propia

Al valorarse la aplicación de las normas ISO 27001 como elemento de control de riesgo el 57 % de los encuestados estaba de acuerdo, mientras que el 6% está en desacuerdo. El 37 % estaría de acuerdo en dejar la gestión anterior del riesgo (ver gráfico 10).

Gráfico 10. Pregunta 6
Fuente: Elaboración propia

Al valorarse la seguridad de un sistema de gestión para las entidades financieras como para la población en general existe un 85 % de acuerdo, 10 % de indecisos y un 5 % en desacuerdo (ver Gráfico 11).

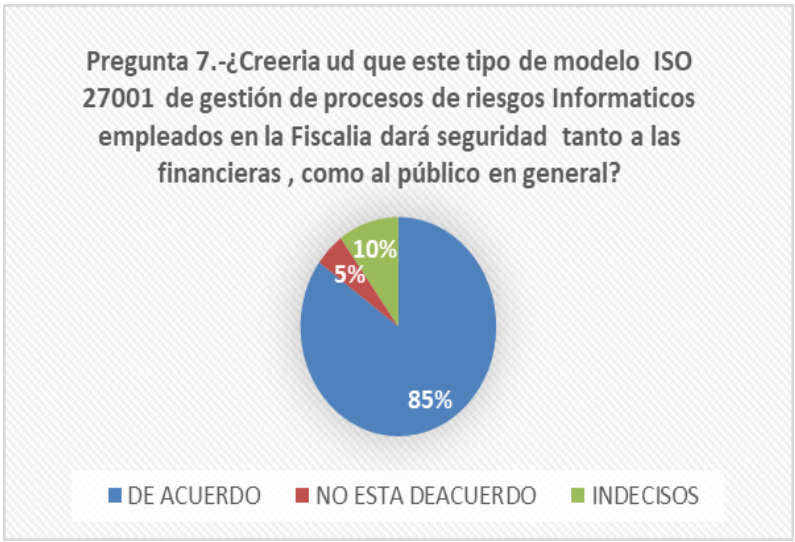


Gráfico 11. Pregunta 7
Fuente: Elaboración propia

Como resultado del análisis de las investigaciones realizadas y el desarrollo de los objetivos de la investigación que se han logrado cumplir tenemos el siguiente resultado para mejorar la calidad del tiempo de servicio de encontrar la culpabilidad de un individuo cuando ha realizado la intromisión por medio electrónicos se podría aplicar un modelo de gestión de riesgos, el cual se acople a las necesidades de la institución en la cual la Fiscalía mejorara los tiempos con el siguiente análisis:

En este análisis se desarrolla primero la ruta de desarrollo de investigación de la Fiscalía con los tiempos requeridos.

Cuadro 1.

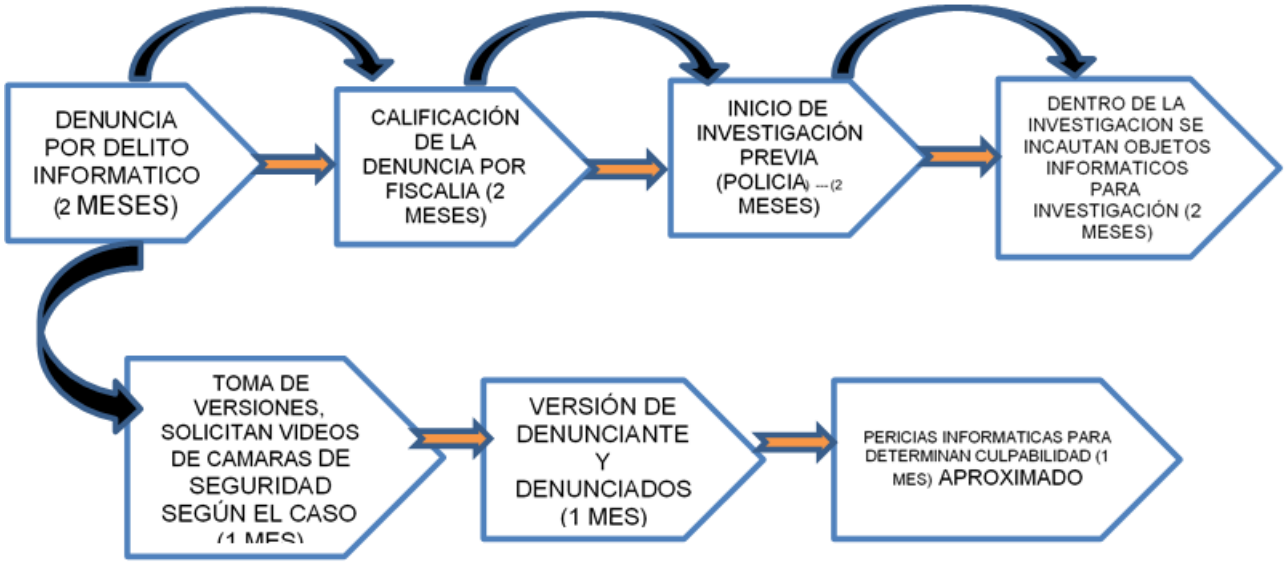


Figura 7.Ruta de procedimiento actual
Fuente: Elaboración propia

Para poder realizar una mejor forma del proceso de gestión en la Fiscalía se lo podría mejorar reduciendo pasos, sin demoras según el modelo ISO 27001.

3.3.2. Aplicación de Procesos de Gestión de Riesgos según ISO 27001 debe de reducir el tiempo de la investigación

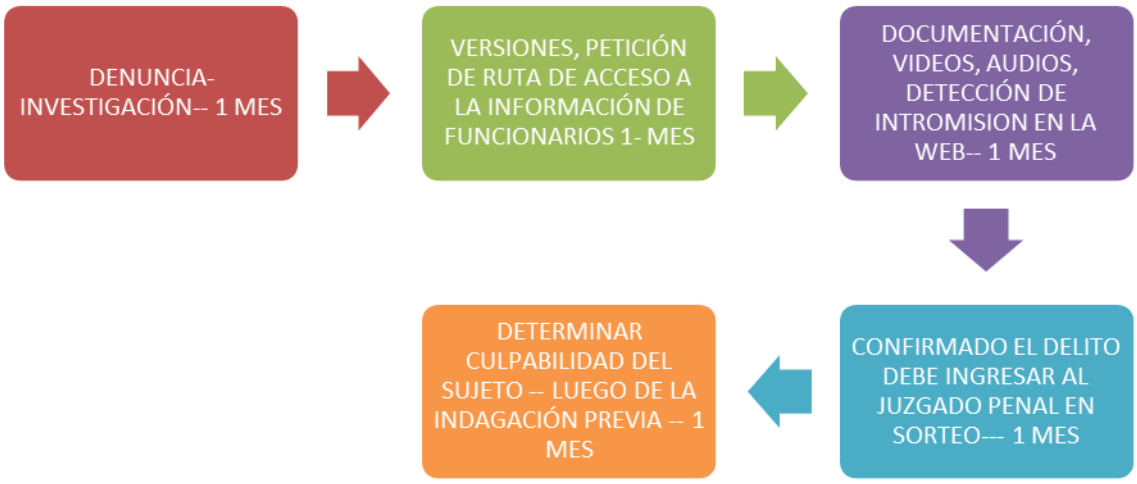


Figura 8.Ruta de proceso con ISO 27001
Fuente: Elaboración propia

Según la figura 8 de la ruta podemos la ruta de los procedimientos que pueda seguir en la Fiscalía General del estado una vez que sr haya simplificado en un proceso sencillo y simplificado donde se unifican los procesos

Como parte final el tiempo al reducir:

ANALISIS
VARIACIÓN DE LA PRODUCTIVIDAD

Tabla 16. *Variación de productividad*

$$\frac{VF - VA}{VA} X\ 100$$

n°	Proceso	Investigación	Flujograma Actual	Flujograma aplicando metodología SIX SIGMA	Resultado (Optimización)	Variación de la productividad
1	Fiscalía proceso actual	Denuncia	2 meses	4 meses	4 meses	12 meses (1 año)
2	Fiscalía si tuviera proceso ISO 27001	Denuncia	2 meses	2 meses	2 meses	6 meses
3			(12 meses -6 meses) *100 / 6 meses		50%	

Fuente: Elaboración propia

En un caso práctico la empresa ASTINAVE es una empresa del sector público, desde 1971 con más de 40 años de experiencia; aportando a nivel operativo para la atención al cliente y su administración, marketing estratégico, y venta de los productos (lanchas patrulleras, lanchas guardacostas, remolcadores, equipos de recolección de lechuguines); y servicio (mantenimiento de embarcaciones, servicios industriales), Fuerzas Armadas y a otras instituciones relacionadas con la seguridad, soluciones, productos y servicios en las siguientes áreas: Comando, Control, Comunicaciones y Computación, Inteligencia, Vigilancia y Reconocimiento (C4IVR), Defensa Electrónica, e Infraestructura de Seguridad de las Información; la cual implemento la norma internacional ISO 27001, en ella se aplicaron los 4 elementos fundamentales de la normativa, como es planificar hacer, verificar, monitorear que ha dado como resultado el mejorar sus procesos y evitar riesgo, vulnerabilidades en la organización luego de haber revisado la literatura de varias certificaciones en

normas de seguridad para evitar riesgos en una institución el modelo ISO 27001; se acopla con los resultados obtenidos en cuanto a la veracidad de los procesos que debe de llevar la fiscalía FGE, la productividad, eficiencia no se mide por el tiempo que se va a dar un resultado sino también a que cada proceso implementado, permita al estado reducir el costo, productivo de cada uno de sus empleados para el estado es un costo adicional el mover el aparato judicial; por cada una de las denuncia presentadas; ASTINAVE llevó un proceso de revisión levantamiento de información que es el mismo que deberá llevar la FGE, para poder realizar estructurales, tanto a nivel físico como tecnológico, ya que con la llegada de la tecnología todo proceso debe ser llevado en línea con transparencia así como las pruebas que se recaben con sus ciertas restricciones este modelo ISO 27001.

No solo se puede aplicar para los delitos informáticos que son los que han tomado su repunte en estos tiempos sino para todos, ya que al mejorar el tiempo de los procesos, disminuir papelería se dará la celeridad necesaria el cual siendo un principio de la FGE, y de algunas instituciones del estado la celeridad procesal, economía procesal son claves para restringir vulnerabilidades; se evaluó el proceso actual que maneja la Fiscalía General del Estado dando como resultado que el proceso toma aproximadamente un año, por cuanto aún tienen un proceso ambiguo, obsoleto como es de recabar aun papelería que en ocasiones se le pierde a la persona que la ingreso; es claro que al automatizar, aplicar la ISO 27001 se reduciría a 6 meses. Es decir que se reduciría en un 50% aproximadamente el tiempo para atender un caso. Por ende, se mejoraría la productividad en resolver los casos por parte de la FGE en Ecuador.

Conclusiones

Se concluye:

- Se recomienda luego del análisis realizado la Fiscalía General del Estado utilice el modelo ISO 27001 el cual tiene una eficiencia en la toma de decisiones dentro de la FGE, tanto en la efectividad de productividad para poder reducir tiempo, costo de tal llamada economía procesal, cada proceso tomara un tiempo indicado, según el indicador de gestión estratégico para mejorar cada uno de los procedimientos de la fiscalía, beneficie de manera sistemática en los presupuestos asignados Fiscalía General del Estado del Ecuador cumplir con los principios, misión y visión de la FGE como son el armonizar, calidad, cantidad, transparencia con el objetivo de sancionar en menor tiempo a quien cometa el delito.

- Se cuantificó el número de ataques cibernéticos al sistema financiero y las inversiones ejecutadas por parte de las entidades financieras para mitigar las perdidas hasta diciembre del 2020. Como resultado, se estableció un modelo de regresión lineal probado con una variable independiente, se explica que el 77,8% de la varianza de la variable dependiente (R^2 de 0.778). Total, las pérdidas de las instituciones financieras por ataques informáticos puede explicarse por los predictores en este caso la variable inversión en infraestructura y sistemas tecnológicos.
- Se catalogó el tipo de ataque informático ejecutado al sistema financiero por delincuencia cibernética y defraudación receptados por la Fiscalía General del Estado. Por lo tanto, la fiscalía respondería con un proceso mejor llevado con documento respalda, Backus necesario, información periódicamente respaldada, antivirus, cortando todos los portales de información para que las entidades bancarias mejoren sus servicios y credibilidad, al tener personal capacitado y calificado, desde los fiscales que puedan verificar el funcionamiento

correcto de los procesos, con la menor manipulación de la información.

- Se propuso elaborar un plan de riesgos donde se evidencia la fortalezas y debilidades de la fiscalía general del estado, que este mismo luego de una análisis se realice una toma de decisión estratégica que no perjudique al usuario, en cuanto la resolución de su caso, viéndolo desde el aspecto de la trazabilidad de los procesos, mejora continua a futuro que el detener el ciberdelito sea rápida y segura con personal calificado que ayude al mantener los principios básicos de la fiscalía: transparencia, celeridad, agilidad confianza, los cuales el modelo ISO 27001, ayudara a TRANSPARENCIA, SEGURIDAD, EFICIENCIA, con capacitación y mejora continua.

Por lo expuesto, se elaboró un modelo de sistemas de información para la medición de los delitos informáticos para la Fiscalía General del Estado, en Ecuador. Por consiguiente, se evaluó el proceso actual que maneja la Fiscalía General del Estado dando como resultado que el proceso toma aproximadamente un año mientras que el nuevo proceso, aplicando la ISO 27001 se reduciría a 6 meses. Es decir que se reduciría en un 50% aproximadamente el tiempo para atender un caso. Por ende, se mejoraría la productividad en resolver los casos por parte de la FGE en Ecuador.

Recomendaciones

- Como primera recomendación para la fiscalía general es que cada proceso que se realice que sea con la menor manipulación de los equipos técnicos, y tecnológicos a pesar de que exista la cadena de custodia, el personal técnico debe realizar respaldo de información o verificar la documentación respalda, de donde se ha dado la infiltración de la información

- Solventar todas las dudas de los usuarios en menor tiempo, es decir, cuando la fiscalía inicia su investigación con carácter de reservado en un lapso de tiempo menor de 2 meses debe de tener ya indicios desde donde se inició el primer ataque, e iniciar por exigir a la entidad que tenía el resguardo de la información que se haga responsable de la misma.

- Al aplicar correctamente un modelo ISO 27001, se debe permitir que el sistema de control que está aplicando la fiscalía se desarrollado, con eficiencia para cuantificar los tiempos como ejemplo de dos fases como es la versión, indagación de los equipos, debe de ser en el menor tiempo disponible con la colaboración de las instituciones y así se hará un trabajo de equipo.

Referencias Bibliográficas

Aggarwal , P., & Arora , P. (2014). Review on cybercrime and security. *International Journal of Research in Engineering and Applied Sciences*, 51-55.

Aguado, C. (2013). Conocer el Balanced Scorecard y los Dashboard. *Marketing Digital y contenidos*, 1-10.

Ajila, A. (2019). *ANÁLISIS JURÍDICO DE LAS LEYES QUE AMPARAN A VÍCTIMAS.* Santo Domingo: Universidad Uniandes.

Allabouche, K., & Diouri, O. (2016). Mobile phones' social impacts on sustainable human development: case studies, Morocco and Italy,. *Entrepreneurship and Sustainability Issues*, 64-73.

Araníbar, J. C. (2008). Inteligencia de negocios. *Scielo*, 101.

Asamblea. (2014). Código orgánico Integral penal. En Asamblea. Montecristi: Asamblea del ecuador.

Bagheri , S., & Ridley , G. (2017). *Organisational cyber resilience: research opportunities. .* Melbourne: Australasian Conference on Information Systems.

Baronienė, L., & Žirgutis, V. (2017). Cybersecurity facets: counterfactual impact evaluation of measure "Procesas LT" in enterprises of the it sector. *Journal of Security and Sustainability Issues, 6*(3), 33-41.

Benavides, C. (2017). Indicadores de calidad de una empresa. *Calidad para Pymes*, 1-10.

Bhatla , T., Prabhu, V., & Dua, A. (2003). *Understandingcreditcardfrauds. Cards Business Review#.* Tata ConsultancyServices.

Bocanegra, S. (2019). *Uso del Dashboard digital para el monitoreo de indicadores de las Unidades de.* Peru: Uniandes.

Bodeau, D., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework.* Bedford: The MITRE Corporation.

Burgos, J. G. (2005). *SISTEMA PARA EL ANÁLISIS DE FRAUDES CON TARJETAS.* Caracas: U. Metropolitana.

Button, M. (2008). *Doing Security: Critical Reflections and an Agenda for Change.* Basingstoke: Palgrave Macmillan.

Caicedo, N. (2015). Metodología para cálculo de un indicador de capacidad de procesos multivariado. *Revista Universitaria Ruta*, 1-10.

Calle, I. I. (2019). *Dashboard Digital para el monitoreo de indicadores y metas de los proyectos.* Peru: Universidad de San martin de saropoto.

Castells, M. (2001). *The Internet Galaxy: Reflexions on the Internet, Business, and Society.* Oxford: Oxford University Press.

Čirjevskis, A. (2016). Sustainability in information and communication technologies' industry: innovative ambidexterity and dynamic capabilities perspectives. *Journal of Security and Sustainability Issues, 6*(2), 27-36.

Conference_Board_of_Canada. (2018). *Building Cyber Resilience.* Ottawa: Conference Board of Canada.

Danzig , R. (2014). *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies.* Washington DC: Center for a New American Security.

Dashtana, Y. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector Atul Bamrara. *International Journal of Cyber Criminology, 7*(1), 96-113.

Dávila, E. (2019). *Cuatro delitos informaticos en el Ecuador.* Guayaquil: Premicias.

Fiscalia. (2019). *Delitos Informaticos.* Guayas: Deloitte.

Fulss, D. C. (Marzo). IMPLANTACIÓN, MANTENCIÓN Y COSO. *MINISTERIO*, 2016.
Garcia, J. (2019). Indicadores de Eficacia y Eficiencia en. *Espacios*, 1-11.
Gavilánez, R. (2017). Análisis de los ataques de hackers a entidades financieras: Una. *JEM*, 1-4.
Global_Cybersecurity_Report. (2017). *Global Cybersecurity Report 2017.* Nexia International Limited.
GONZÁLEZ, E. A. (2017). *ESTAFA INFORMÁTICA DEL ARTÍCULO.* sevilla: u. sevilla.
Gonzalez, H. (2019). INDICADORES CONFIABLES PARA SISTEMAS DE GESTIÓN. *Calidad & Gestión*, 1-10.
Granda, K. L. (2020). ATAQUES CIBERNÉTICOS EN LAS INSTITUCIONES FINANCIERAS. *OBEPEMS*, 1-5.
Guerrero, G. (2019). Business Intelligence: ¿Qué tipo de dashboard es el ideal para tu organización? *Inclussion cloud computing*, 1-10.
Hathaway, M. (2018). Gestión del Riesgo. *Cibernetico Nacional*, 1-22.
Holling, C. (1973). Resilience and stability of ecological systems. *Annu Rev Ecol Syst, 4*, 1–23.
Huescas, O. J. (2011). Metodología de la Investigación. *Editorial Mc Graw Hill, Cuarta edición.*, 1-2.
Hugo Bayardo Santacruz1, M. M. (2019). Los delitos informáticos y su tipifcación en la. *risti*, 1-11.
Interior, M. d. (2019). *Plan estrategico de seguridad pública.* Quito: Policia.
Jankalová, , M., & Jankal, R. (2017). The assessment of corporate social responsibility: approaches analysis, Entrepreneurship and Sustainability Issues . *Entrepreneurship and Sustainability Issues , 4*(4), 441-459.
Kriviņš, A. (2015). Towards security and safety: police efficiency across European countries. *Journal of Security and Sustainability Issues, 5*(1), 35–44.
Kuehl, D. (2009). From cyberspace to cyberpower: defining the problem. En F. Kramer, & S. Starr , *Cyberpower and National Security.* (págs. 1–17). Washington DC: National Defense University Press.
Law, D. (11 de Diciembre de 2018). *Paneles Arcgis*. Obtenido de https://www.esri.com/arcgis-blog/products/ops-dashboard/analytics/make-your-dashboards-more-dynamic-using-url-parameters/
Linkov , I., & Eisenberg , D. (2013). Measurable resilience for actionable policy. *Envir Sci Tech, 47*, 108–110.
Lux, L. M. (2020). El delito de fraude informático: concepto y delimitación. *Scielo*, 1-10.
Maes, S., Tuyls, K., & Vanschoenwinkel, B. (2002). *Credit carddetectionusingBayesian and neuralnetworks.* Proceeding International NAISO Congress on neuronfuzzy Technologies.
Martinez, D. (2017). *Metodologia para el diseño de dashboard orientado al registro de evidencias.* Puyo: Unir.
Medrano, J. Á. (2015). Decisiones estratégicas, decisiones operativas. *Los cinco anillos de Musashi*, 1-10.
Minn Wu, R. (2019). *Do Security Toolbars Actually Prevent Phishing Attacks?* Cambridge: MIT Computer Science and Artificial Intelligence.
Morín, E. (2017). Indicadores de rentabilidad. *Cepec*, 1-10.
Muguira, A. (2019). Dashboard Operativo. *Tu Dashboard*, 1-10.
Munteanu, C., & Tamošiūnienė, R. (2015). Modern approaches in quantifying economic security. Case study of Estonia, Latvia, Lithuania and Republic of Moldova. *Journal of Security and Sustainability Issues, 4*(4), 596-610.
Oliveira, W. (2018). Indicadores de rendimiento de Kpi. *Heflo*, 1-10.
Padmavathi, U. (2013). A survey on various cyber-attacks and their classification. *International Journal of Network Security, 15*(5), 390- 396.
Pettersson, M. (2012). *Banks likely to remain top cybercrime targets.* Denver: Symantec Corporation, Excutive Report.
Polo, D. (2020). Indicadores de productividad. ¿Cuándo medir? *Gestionar Fácil*, 1-10.

Ramírez, F. C. (2017). RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN. *Financial Stability Board*, 1-5.
RAMÍREZ, J. J. (2019). *ANÁLISIS DE LA TAXONOMÍA DE LOS DELITOS INFORMÁTICOS EN EL.* 2019: ug.
Ramos, S. (2017). Hechos y Dimensiones: Modelado Dimensional. *SolidQ*, 1-10.
Rocamora, J. (2020). Cómo crear un cuadro de mando o dashboard para eCommerce (y cómo usarlo bien). *Marketing Ecommerce*, 1-10.
RODRÍGUEZ-CRUZ, Y. (2016). Requerimientos informacionales para la toma de decisiones. *Scielo*, 1-16.
Roncancio, G. (2019). Indicadores de Gestión (KPI's): Tipos y Ejemplos. *Pensemos*, 1-10.
Sanz, H. (2015). *Diseño e implementación de un cuadro de mando de portal inmobiliario.* España: Universidad de catalunya.
Siklos, P. (2001). *Money, banking and financial institutions:.* Otawa: Canada in the global environment.
Stahlberg, M. (2009). *Patent Application Publication Malware Detection.* Delaware.
Štitilis, D., Pakutinskas, P., & Kinis, U. (2016). Concepts and principles of cyber security strategies,. *Journal of Security and Sustainability Issues, 6*(2), 197-210.
Štitilis, D; Klišauskas, V. (2015). Aspets of cybersecurity: the case of legal regulation in Lithuania,. *Journal of Security and Sustainability Issues, 5*(1), 45–57.
Štitilis, D; Pakutinskas, P; Kinis, U. (2016). Concepts and principles of cyber security strategies,. *Journal of Security and Sustainability Issues, 6*(2), 197-210.
Swanda, P. (2010). *myaccountingcourse*. Obtenido de myaccountingcourse: https://www.myaccountingcourse.com/accounting-dictionary/financialinstitution
Vera, A. H. (2019). *LA SUPLANTACIÓN DE IDENTIDAD CIBERNÉTICA EN EL ECUADOR.* Colombia: Universidad externado Colombia.
Yahma, D. (2015). *National Cyber security policy framework for South Africa.* Government Publication.
Zumárraga., F. d. (11 de Septiembre de 2002). *Tesis Doctoral.* Ambato: Universidad de Ambato. Recuperado el 05 de 01 de 2018, de http://cv.uoc.edu/web/~ddoctorat/treballs/2002/dret/fquinto.pdf

ANEXOS

Anexo 1. Matriz Auxiliar para el Diseño de la Investigación

VIII. ANEXOS

Anexo 1: Matriz Auxiliar para el Diseño de la Investigación

		Operacionalización de las variables			
Problemas	**Objetivos**	**VI y VD**	**Variables empírica**	**Indicadores**	**Ítems**
			VE		**VI**
La mala identificación de los cybercrimenes catalogarlos como un delito de apropiación fraudulenta cuando la gama de delitos informáticos son varios con diversas características, de una falsa de seguridad en la web para los usuarios en cuenta sus cuentas virtuales	• Definir los sustentos teóricos, jurídico, metodológico, práctico para el desarrollo de un modelo de seguridad de la información para la medición de los delitos informáticos para la Fiscalía General del Estado, en Ecuador		Identificar que factor influye en la detección de la amenaza	Tiempo estimado para detección	¿Cuál es el tiempo estimado para la detección del virus en las instituciones?
			Mostrar de qué modo opero el delito informático	Tiempo estimado evolución de la amenaza	Cuánto tiempo le tomaría a la fiscalía para verificar si es una amenaza o vulnerabilidad
			Viabilidad para verificar el delito ocurrido según el COIP	Tiempo de efectividad de para detectar amenazas	¿Cuál es el porcentaje de efectividad de para detectar amenazas?
			Analizar puntos críticos de la institución para los delitos informáticos	Cantidad de delitos que más se desarrollan en las entidades financieras	¿Cuáles son los delitos que más se desarrollan en las entidades financieras

		Variables Independientes	Verificar que se cumplan las normas de seguridad informática en cuanto a los delitos informáticos	Cantidad tipos de delitos informáticos según el COIP	¿Cuáles son los tipos de delitos según el COIP?
✓ Los parámetros requeridos en los procesos de transacciones en línea no son seguros ya que los hackers, crackers, entre otros que tienen diferente manera de delinquir y de adquirir de manera fraudulenta dinero, y el no contar con políticas, estándares de estrategias para disminuir los casos dicho establecer parámetros de ejecución de los procesos para transacciones diarias en las instituciones financieras que son un riesgo para la economía de los clientes.	✓ • Cuantificar el número de ataque cibernéticos al sistema financiero se han generado hasta diciembre 2020, relacionado a delincuencia cibernética y defraudación receptados por la Fiscalía General del Estado	Realizar la evaluación y el tratamiento de riesgos	**VEID**		¿Cuál es la cantidad de tiempo que dispone la fiscalía para resolver un caso?
		Plan de tratamiento del riesgo	Costear las perdidas por delito informático	Cantidad de tiempo que dispone la fiscalía para resolver un caso	¿Cuáles son los puntos críticos para resolver un delito informático según el eso 27001?
			Identificar amenaza y vulnerabilidad	Cantidad de puntos críticos para resolver un delito informático según la ISO 27001	¿Cuál es la Cantidad de tiempo para el cumplimiento de la normas ISO?
			Determinar si las empresas aplicaron en su debido tiempo de aplicación de las fases	Cantidad de cumplimiento de la normas ISO	¿Cuál es la cantidad de pérdida estimada de las instituciones financieras?
Los sistemas de seguridad en las diversas instituciones sean estas con fines de lucro o no están expuestas a la ciberdelincuencia debido a la mal manejo de la seguridad de las bases de datos, servidores que son los más vulnerables.	✓ • Catalogar el tipo de ataque informático ejecutado al sistema financiero por delincuencia cibernética y defraudación receptados por la Fiscalía General del Estado		Cuantificar al Personal que tenga la capacidad de verificar la vulnerabilidad y la amenaza	Cantidad de tiempo estimado de perdida de instituciones financieras	
		Variable Dependiente	Al tener un mejor personal la fiscalía podrá realizar mejores investigaciones rápida y eficaces	Cuáles son los riesgos que corre una institución financiera por los delitos	¿Cuáles son los riesgos que corre una institución financiera por los delitos?
		Gestión de procesos de riesgo cibernético en el sector financiero	Evaluar tiempo de duración de la denuncia de delito informativo	Cantidad de tiempo se deberían de aplicar las ISO 27001	

	• Proponer un modelo de sistemas de información para la medición de los delitos informáticos para la Fiscalía General del Estado, en Ecuador		Viabilidad para verificar el delito ocurrido según el COIP		
			Verificar número de delitos denunciados en la Fiscalía		¿Cuantos es la Cantidad de días toma la fase de la ISO 27001?
			Evaluar tiempo de duración de la denuncia de delito informativo	En cuanto tiempo la fiscalía debería de tener resultados si cambia sus sistema de investigación y procesos de los delitos informáticos	
			Resolver delito informático duración		
El no contar con la debida protección de datos de información cifrada que pueda mantener el anonimato de los valores que se encuentran en las cuentas de los usuarios es el centro de la atención de los delitos de cuello blanco, ya que no son contabilizados si no a través de un engorroso papeleo que se realiza entre demandas al banco, pruebas y demás que duran hasta un año y medio para la devolución al cuenta ahorrista, siendo fácilmente presas de estos Delincuente informático			Analizar puntos críticos de la institución para los delitos informáticos		¿Cuál es la Cantidad de personal capacitado se debe tener para que la amenaza sea detectada?
			Verificar que se cumplan las normas de seguridad informática en cuanto a los delitos informáticos		
			Costear las perdidas por delito informático		¿En cuánto tiempo la fiscalía debería de tener resultados si cambia su sistema de investigación y procesos de los delitos informáticos?
			Identificar amenaza y vulnerabilidad		
			Controlar el Tiempo de aplicación de las normas por institución		

Anexo 2. Descripción de variables

Anexo 4: Descripción de variables

Variable	Indicadores	Objetivo	Unidad	Fórmula	Tipo de Variable	Ítems	Frecuencia	Técnica	Instrumento	Fuente
Realizar la evaluación y el tratamiento de riesgos	Tiempo de detección del tipo de vulnerabilidad o amenaza	Identificar que factor influye en la detección de la amenaza	Días	Tiempo estimado para detección	Analítica	¿Cuál es el tiempo estimado para la detección del virus en las instituciones?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
	Desarrollo del delito en la entidad financiera	Mostrar de qué modo opero el delito informático	Días	Cantidad de delitos que más se desarrollan en las entidades financieras	Analítica	¿Cuáles son los delitos que más se desarrollan en las entidades financieras	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
Plan de tratamiento del riesgo	Encasillar la amenaza o vulnerabilidad, según el tipo de delito del COIP	Viabilidad para verificar el delito ocurrido según el COIP	Días	Cantidad tipos de delitos informáticos según el COIP	Analítica	¿Cuáles son los tipos de delitos según el COIP?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
	Verificar los puntos critico de los delitos	Analizar puntos críticos de la institución para los delitos informáticos	Analizar	Cantidad de puntos críticos para resolver un delito informático	Analítica	¿Cuáles son los puntos críticos para resolver un delito informático	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria

				según la ISO 27001		según la ISO 27001?				
	Porcentaje de cumplimiento de las normas para que no se realicen los delitos informáticos	Verificar que se cumplan las normas de seguridad informática en cuanto a los delitos informáticos	Porcentaje	Cantidad de cumplimiento de la normas ISO	Analítica	¿Cuál es la Cantidad de tiempo para el cumplimiento de la normas ISO?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
Hacer funcionar el SGSI	Porcentaje de pérdidas de la instituciones financieras por los delitos informáticos	Costear las perdidas por delito informático	Porcentaje	Cantidad de tiempo estimado de perdida de instituciones financieras	Analítica	¿Cuál es la cantidad de pérdida estimada de las instituciones financieras?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
	Tipos de riesgos a cubrir por las instituciones	Identificar amenaza y vulnerabilidad	Cantidad	Los riesgos que corre una institución financiera por los delitos	Analítica	¿Cuáles son los riesgos que corre una institución financiera por los delitos?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria

	Desarrollo del tiempo de fases de la ISO	Determinar si las empresas aplicaron en su debido tiempo de aplicación de las fases	Días	Cantidad de Días toma la fase de la ISO 27001	Analítica	¿Cuántos es la Cantidad de días toma la fase de la ISO 27001?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
Implementación de controles y procedimientos obligatorios	Cantidad de personal capacitado para identificación de vulnerabilidades. O amenazas	Cuantificar al Personal que tenga la capacidad de verificar la vulnerabilidad y la amenaza	Cantidad	Cantidad de personal capacitado se debe tener para que la amenaza sea detectada	Analítica	¿Cuál es la Cantidad de personal capacitado se debe tener para que la amenaza sea detectada?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria
	Control de cambios en la fiscal para detección de delitos informáticos	Al tener un mejor personal la fiscalía podrá realizar mejores investigaciones rápida y eficaces	Cantidad	Tiempo la fiscalía debería de tener resultados si cambia sus sistema de investigación y procesos de los delitos informáticos	Analítica	¿En cuánto tiempo la fiscalía debería de tener resultados si cambia su sistema de investigación y procesos de los delitos informáticos?	Semanal	Estadística, Análisis Documental	Base de datos, investigación, Bibliografía	Primaria, Secundaria

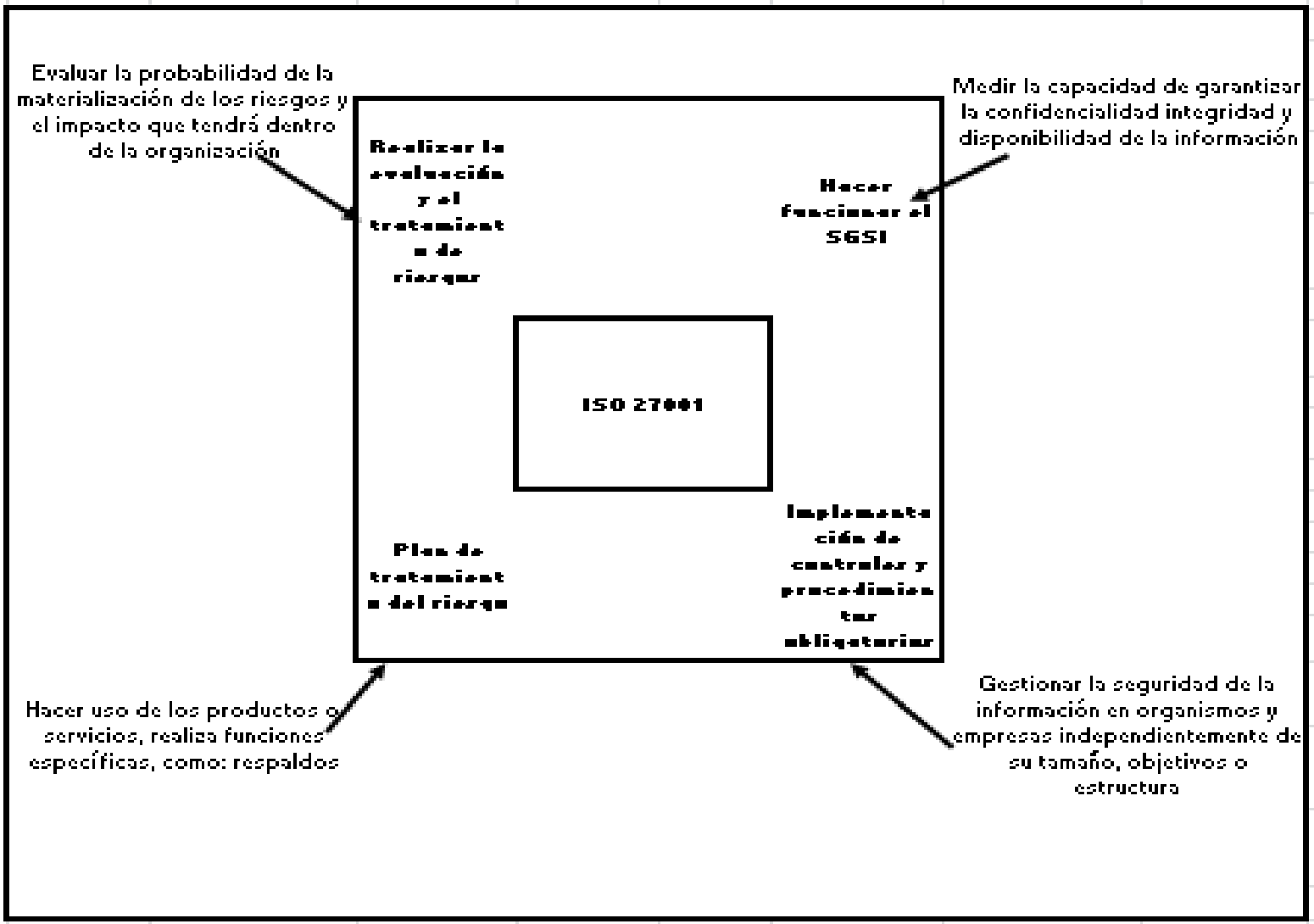
Anexo 3. Autores de marco teórico Variables

Anexo 3: Autores de Antecedentes del Marco Teórico Variables, Dimensiones e Indicadores

Variable	Descripción de la Variable	Nombre del autor que aporta conceptos	Año de publicación
Realizar la evaluación y el tratamiento de riesgos	*Permitirá a la dirección de la empresa tener la visión necesaria para definir el alcance y ámbito de aplicación de la norma, así como las políticas y medidas a implantar, integrando este sistema en la metodología de mejora continua	Vidalita De Freitas	2009
	sistemas de gestión definen el riesgo como el efecto que genera la incertidumbre, puede ser positivo o negativo, debido a la falta de información de la situación, proceso o procedimiento	César Augusto Berríos Masía	2015
	Evaluar la probabilidad de la materialización de los riesgos y el impacto que tendrá dentro de la organización	Javier Esa Quispe Loarte	2018
Plan de tratamiento del riesgo	Medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI	Jorge Luis Valdivieso Troya	2015
	Medir el impacto en una base de severidad, basada en el valor de la perdida monetaria	Aníbal Mantilla Guerra	2009
	Medir la capacidad de garantizar la confidencialidad integridad y disponibilidad de la información	Andrea Murillo Chiriboga	2017
Hacer funcionar el SGSI	Hacer una pausa y definir procesos y procedimientos como consecuencia, de lo que se debe de hacer , cuando, hacerlo	Sara Cuervo Álvarez	2017
	Plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los	Alejandro Jiménez Leído Ximena Salazar Barrera	2016

	riesgos de seguridad de la información		
	Hacer uso de los productos o servicios, realiza funciones específicas, como: respaldos de información de los equipos de los colaboradores, gestión del licenciamiento para las estaciones de servicios, servidores y la gestión de la mesa de ayuda	Julio Cesar Pilla Yanzapanta	2019
Implementación de controles y procedimientos obligatorios	personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarios	Ángel Hidalgo	2018
	personal que se van a dedicar a implantar y mantener el sistema	Mar Martínez Carrascosa	2019
	gestionar la seguridad de la información en organismos y empresas independientemente de su tamaño, objetivos o estructura	Guillermo Bustamante Moyano	2020

Anexo 4. Cuadro de la ISO 27001



Anexo 5. FORMATO DE ENCUESTA MODELO ISO 27001---FISCALIA

Pregunta 1.- ¿A través de qué medios han detectado amenaza o vulnerabilidad informática?	
Celulares	
Computadoras	
Redes Sociales	
Links a través de la red	

Pregunta 2.- ¿En qué entidades financieras ha tenido mayor cantidad de denuncias por delitos informáticos?	
Bancarias	
Mutualistas	
Cooperativas de Ahorro y Crédito	
Ninguna	

Pregunta 3.- ¿Cree Ud. que la gestión de procesos en los delitos informáticos de la fiscalía general de estado es?	
	SI
Ágil	
Oportuna	
Lenta	

Pregunta 4.- ¿Cree Ud. que si se desarrolló un modelo de gestión de proceso como el ISO 27001, Cuánto tiempo duraría investigación en Fiscalía?	
1 año	
2 años	
6 meses	

Pregunta 5.- ¿Cuáles son los riesgos informáticos más comunes que ha escuchado a las instituciones financieras?	
Estafa por medios electrónicos	
Fraude por medios electrónicos	
Clonación de tarjetas de crédito o debito	

transferencia de dinero por medios electrónico	

Pregunta 6.- ¿Si se maneja un plan de riesgo en las entidades financieras ayudara a mejorar el proceso determinación de culpabilidad?	
DE ACUERDO	
NO ESTA DE ACUERDO	

Pregunta 7.- ¿Estaría Ud. desacuerdo se integra un plan de riesgos dentro de las instituciones financieras aplicando ISO 27001 Como gestión de control de riesgos?	
De acuerdo	
No esta desacuerdo	
Dejaría la gestión anterior para detección de riesgo informáticos	