UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"GUÍA DE GESTIÓN DE RIESGOS CIBERNÉTICOS PARA EMPRESAS DEDICADAS A BRINDAR SERVICIOS DE AUDITORIA EXTERNA EN EL ÁREA METROPOLITANA DE SAN SALVADOR"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR GRUPO S51:

GARCÍA HENRÍQUEZ, MAYRA ALEJANDRA

PÉREZ GONZÁLEZ, YESSICA ROXANA

RODRÍGUEZ FUENTES, YESENIA PATRICIA

PARA OPTAR AL GRADO DE:

LICENCIADA EN CONTADURÍA PÚBLICA

ASESOR ESPECIALISTA:

JOSÉ FELIPE MEJÍA HERNÁNDEZ

DICIEMBRE DE 2019

SAN SALVADOR, EL SALVADOR, CENTROAMERICA.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

AUTORIDADES UNIVERSITARIAS

Rector	:	Máster Roger Armando Arias Alvarado
Secretario General	:	Máster Cristóbal Hernández Ríos Benítez
Decano de la Facultad de Ciencias Económicas	:	Lic. Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas	:	Licda. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	:	Licda. María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador General de Procesos de Graduación Facultad de Ciencias Económicas	:	Lic. Mauricio Ernesto Magaña Menéndez
Coordinador de Seminario de Procesos de Graduación de la Escuela de Contaduría Pública	:	Lic. Daniel Nehemías Reyes López
Docente director	:	Lic. José Felipe Mejía Hernández
Jurado evaluador		Lic. José Felipe Mejía Hernández
	:	Licda. María Margarita de Jesús Martínez Mendoza de Hernández
		Lic. Héctor Alfredo Rivas Núñez

DICIEMBRE DE 2019

SAN SALVADOR, EL SALVADOR, CENTROAMERICA.

AGRADECIMIENTOS

A Dios por apoyarme en todo momento, a mis padres Mario y Guillermina que son los motores de mi vida y que con amor y sacrificio siempre me brindaron su apoyo. A mi hermano Daniel porque es una pieza fundamental para el logro de este sueño. Sin dejar a un lado a personas especiales que me brindaron su ayuda incondicional Carmen Bautista, Stefany Flores y los esposos Chacón y familia. Y por último a todos los docentes que contribuyeron a mi formación académica, a mis compañeros y amigos; y en especial a Yesenia y Yessica que con su esfuerzo, sacrificio y dedicación hemos culminado juntas este sueño.

Mayra Alejandra García Henríquez

A Dios por ser mi guía y llenarme fuerzas para lograr mi objetivo, a mis padres Blanca y Juan pilares fundamentales en mi vida, que con mucho amor y sacrificio siempre estuvieron dispuestos a brindarme su apoyo incondicional para hacer realidad mis sueños. A una persona muy importante, Rony, que siempre estuvo pendiente de mí, animándome para seguir adelante, a cada uno de los maestros que han contribuido con dedicación en mi formación profesional y a Yesenia y Mayra porque con trabajo en equipo, responsabilidad y amistad hemos culminado el trabajo de investigación con éxito.

Yessica Roxana Pérez González

Quiero agradecerle primeramente a Dios, porque me brindo la sabiduría necesaria para alcanzar mis metas, a mis padres Teresa y Carlos por todo su apoyo que me brindaron desde sus posibilidades económicas me otorgaron los recursos necesarios para continuar con mis estudios, y a mi familia en general. A mis compañeras de trabajo de investigación que gracias a su compromiso y dedicación estamos cumpliendo uno de nuestros mayores sueños, y a todos aquellos los que me animaron a nunca abandonar mis sueños.

Yesenia Patricia Rodríguez Fuentes

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

La velocidad de los cambios tecnológicos, la popularización de nuevos dispositivos, nuevas formas de procesamiento de datos y las posibilidades de conexión remota han propiciado la proliferación de acciones delictivas en el ciberespacio, por lo que ningún dispositivo complejo o sencillo está exento de ser atacado.

Con la finalidad de proteger la información de las firmas de auditoría de las amenazas del ciberespacio se realiza la Guía de Gestión de Riesgos Cibernéticos para las Firmas de Auditoría, que sugiere la creación de un comité de ciberseguridad para la implementación de la presente guía.

La Guía Gestión de Riesgos Cibernéticos se enfoca en la prevención, protección, detección, respuesta y comunicación; recuperación y aprendizaje, como medidas de control de seguridad que ayuden a disminuir el impacto ante posibles eventos que afecten la confidencialidad, integridad y disponibilidad de la información.

Es una herramienta alternativa para gestionar los riesgos cibernéticos, mediante la implementación de una serie procedimientos de identificación, evaluación y respuesta al riesgo.

En la investigación se utilizó el método cualitativo que se enfoca en comprender los fenómenos explorándolos de manera inductiva debido a que por medio del acercamiento a la unidad de análisis empleando técnicas de observación, anotación y entrevistas al gerente de tecnología de la información y comunicación y al auditor socio de la firma de auditoria en análisis. Para ello se hizo uso de la técnica de la entrevista y el cuestionario como instrumentos de recolección de datos que se analizaron para comprobación de la hipótesis. La información se obtuvo de una firma de auditoría del área metropolitana de San Salvador; además se recabó información de noticias, informes, notas y revistas. Obtuvieron los siguientes resultados:

Los auditores y gerentes de TI tienen conocimiento acerca de que los avances tecnológicos proporcionan ventajas que se deben aprovechar y riesgos que mitigar por lo que se han establecido algunos procedimientos encaminados a la seguridad de la información, pero existen deficiencias en cuanto a la ciberseguridad debido a que es un área poco conocida, como consecuencia la entidad se vuelve vulnerable y expuesta a amenazas potencialmente dañinas.

Se manifiesta la disposición de inversión y la disponibilidad de la implementación de la guía de gestión de riesgos cibernéticos para estar preparados ante los riesgos del ciberespacio.

Para que las firmas de auditoría puedan ejercer una gestión de manera completa y eficaz se recomienda incluir en la gestión estratégica el riesgo cibernético la creación de un comité de ciberseguridad que coordine los esfuerzos en esta materia e implementar la Guía de Gestión de Riesgos Cibernéticos de manera que ayuden a la protección de la información propia y de los clientes.

INTRODUCCIÓN

Los cambios tecnológicos plantean nuevas oportunidades y retos para las firmas de auditoría en El Salvador. La existencia de un mundo virtual en donde personas, software y los servicios de internet interactúan (ciberespacio), no solo genera un impacto a la organización; sino, sobre terceros interesados. Por lo tanto, saber gestionar los posibles riesgos que esto trae consigo es una labor en la que debe verse involucrada cada uno de los que conforman la organización.

Por tal motivo la investigación está enfocada en brindar una herramienta con lineamientos y controles claves que puedan implementarse; de igual modo permitir crear un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Con la finalidad que se pueda ajustar a las necesidades de cada firma de auditoría.

El desarrollo de esta investigación se divide en 4 capítulos que son:

El capítulo 1 contiene el planteamiento del problema, que describe los antecedentes de la situación problemática, delimitación del problema, justificación y objetivos de la investigación.

En el capítulo II se integra por la situación actual de las firmas de auditoría, caso conocido de ataque cibernético, así como los principales aspectos legales y normativos aplicables.

El capítulo III detalla la metodología de la investigación aplicando estrategias, métodos y técnicas para la obtención de resultados del proceso de investigación.

Finalmente, el capítulo IV describe la propuesta de solución para contribuir en la gestión de riesgos cibernéticos en las firmas de auditoría dándoles una respuesta inmediata. Se debe: (a) apostar a una infraestructura moderna y segura; (b) contar con talento humano capaz de comprender las amenazas, riesgos, retos y oportunidades del ciberespacio; y (c) legislación y regulación aplicables a los delitos cibernéticos.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1. Antecedentes del problema

Las Tecnologías de la Información y Comunicación (TIC), surgen en un contexto de creciente necesidad de contar con herramientas que faciliten el intercambio de información, comunicación, medios para hacer negocios, acceso a conocimientos e innovación; ante los cuales el ser humano ha buscado mecanismos para adaptarse; ya que, el mundo experimenta constantes cambios.

El punto de referencia para la problemática en estudio, fue la aparición de las primeras computadoras desde la "máquina analítica (analytical engine) creada por Babbage a finales de la década de los años 40" (M/olero, 2016, pág. 16), hasta las computadoras modernas del año 2019. Por otra parte, el surgimiento de internet y redes inalámbricas, hizo posible que un gran número de personas de diferentes países se interconecten.

De acuerdo al informe de ciberseguridad del Banco Interamericano de Desarrollo (BID, 2016) "América Latina y el Caribe es la región donde más de la mitad de su población tiene conectividad a internet y la tasa de crecimiento de usuarios se encuentra entre las más altas del mundo", disminuyen las barreras de comunicación y se generan nuevas oportunidades de negocios a nivel nacional e internacional que impulsan el crecimiento económico.

Es por ello que las firmas de auditoría que están a la vanguardia incluyen las TIC a su idea de negocio, con la finalidad de: (a) incrementar su productividad y optimizar servicios; (b) minimizar costos y/o agilizar procesos que permitirá contar con información oportuna; (c) mejorar la comunicación con los clientes; y (d) otros beneficios. Pero esto implica asumir que la información que se transmite está expuesta a riesgos, amenazas y vulnerabilidades; ante esto, es conveniente se tomen medidas de gestión de la información, en aspectos como seguridad de la información o seguridad informática.

Sin embargo, a principios de los años 2000 surgen indicios del desarrollo de una dimensión poco conocida que vincula el mundo físico y digital denominado ciberespacio; en el cual, circula una gran cantidad de datos atractivos para los ciberdelincuentes. En consecuencia, es primordial que las firmas de auditoría cuenten con medidas de seguridad cibernética apropiada.

Es por eso que conforme las TIC han ido evolucionando, diversos organismos internacionales vieron la necesidad de crear marcos de referencia, los cuales pueden ser adoptados por empresas de diferentes países ajustándose al entorno empresarial dinámico. Con base en políticas y normativas sobre ciberseguridad, que han implementado Gobiernos Centrales, por ejemplo, el Consejo Nacional de Política Económica y Social de la República de Colombia, donde el departamento nacional de planeación emite lineamientos de política para ciberseguridad y ciberdefensa, con el propósito de:

> Desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas (…) a razón de la creciente capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías, para generar amenazas informáticas ya que constituyen una preocupación común entre los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil. (CONPES Colombia, 2011, págs. 2,4)

El perfil de El Salvador, tanto para el informe de la Unión Internacional de Telecomunicaciones (ITU) como para el BID, evidencia la intención de El Salvador por colocar la ciberseguridad como un tema de agenda nacional, además de destacar los esfuerzos por establecer una legislación específica para estos delitos (FEPADE, 2017, pág. 66). Es por ello que con la cooperación de parte del Gobierno de Corea y el Banco Eximbank de Corea, ejecutaron un proyecto de intercambio de conocimiento para la protección de infraestructura crítica en El Salvador y la mejora de la ciberseguridad cuyo objetivo fue aportar conocimientos y establecer un marco de referencia para

que El Salvador pueda implementar un mecanismo de protección e identificación de infraestructura crítica para reforzar las medidas en dicho tema.

Aparte de ello en materia de normativa técnica se cuenta con la creación del Organismo Salvadoreño de Normalización y con un Capítulo ISACA en San Salvador cuyo objetivo es "dar servicio a sus socios e interesados de la región organizando seminarios, eventos y talleres locales con temas sobre riesgos y controles de auditoría, ciberseguridad, gobierno de TI y seguridad de información" (ISACA, 2019). Sin embargo, los esfuerzos no son suficientes existen deficiencias en cuanto a normativa técnica y leyes que regulen las actividades que se realizan en el ciberespacio.

1.2. Caracterización

En un entorno cada vez más digital, en donde existe una mayor interacción entre personas, *software*, internet, conexión de redes y dispositivos; la seguridad y privacidad de la información que se maneja en las firmas de auditoría se podría ver comprometida o expuesta ante prácticas de ciberdelincuencia, *ciberactivismo, hacktivismo, malware e* ingeniería social; además de vulnerabilidades que un usuario malintencionado después de obtener conocimiento de ellas intentara explotarlas con diversos fines; al acto de explotación de una vulnerabilidad mediante el uso de técnicas y programas se le conoce como ataque.

Frente a este panorama es importante mencionar que existen una serie de limitantes que poseen los líderes de las firmas de auditoría respecto a la protección de la información almacenada y que interactúa en el ciberespacio.

Generalmente las firmas no conciben o ven lejano convertirse en un blanco atractivo para los cibercriminales; es por ello que en ocasiones que un ciberataque se valore como un riesgo de poca trascendencia, por esta razón pocas firmas de auditoría cuentan con políticas de seguridad cibernética o están desfasadas, puesto que los controles que poseen se enfocan en problemas

pasados; la falta de esfuerzos técnicos y económicos es otra de las limitantes pues en muchos casos no cuentan con presupuesto para contratar personal capacitado o capacitar a los empleados; agregando que estos algunas veces poseen malos hábitos de seguridad que permiten a los atacantes introducirse a los sistemas de información.

Cabe resaltar que en el *software* las vulnerabilidades son la causa principal de robo de datos ya que generalmente se introducen por errores en el sistema operativo o el código de aplicación. Productores como Microsoft y Apple lanzan parches y actualizaciones cuando descubren una vulnerabilidad; simultáneamente los atacantes buscan descubrirlas antes y aprovecharse de estas; práctica conocida como ataque de día cero.

> Otra de las vulnerabilidades son del hardware que se presentan a menudo mediante defectos de diseño de la memoria RAM, por ejemplo, consiste básicamente en capacitores instalados muy cerca unos de otros, debido a la cercanía, los cambios constantes aplicados a uno de estos capacitores podían influir en los capacitores vecinos, ralentizando las computadoras. (Cisco Networking Academy, 2019)

Aparte de ello la información puede estar expuesta y vulnerable ante las prácticas de ingeniería social, ya que, esta usa técnicas de engaño y manipulación que fácilmente pueden confundir al recurso humano para que divulgue información confidencial, pues el atacante se presenta por medio de una página web o un correo malicioso solicitando datos personales, financieros o de un cliente de la firma de auditoría, por lo que resulta imperante que conozcan indicios de un posible robo de datos, para no sufrir las consecuencias de perder información valiosa de la firma y de los clientes.

El acceso a la información por personas no autorizadas por medio del empleo de diversas técnicas y el aprovechamiento de vulnerabilidades trae consigo consecuencias a las que se debe

prestar atención; por ejemplo, si en la firma de auditoría un atacante logra obtener toda la información financiera, fiscal y/o comercial de un cliente habitual, este perderá la confianza en los servicios que se le ofrecen, la noticia posiblemente se divulgue por diferentes medios de comunicación , en consecuencia los demás clientes desconfiaran de los servicios ofrecidos; se verá afectada su reputación e imagen por lo que se puede generar dificultades para obtener de nuevos clientes o mantener los ya existentes. Agregando que el cliente podría sufrir pérdidas y optaría por interponer una demanda por daños y perjuicios, o de lucro cesante; ahora será necesario destinar esfuerzos técnicos y económicos al proceso jurídico; los ingresos de la firma se reducirían considerablemente por lo que los empleados se pueden ver afectados destituyéndolos de sus puestos o reduciendo horario laboral, las ganancias disminuyen considerablemente y surgen los problemas financieros que en algunos casos conducen a la quiebra y cierre del negocio.

En conclusión, resulta importante que en las firmas de auditoría cuenten con una guía que les permita gestionar los riesgos cibernéticos, y resguardar la información ante prácticas cibercriminales cuyo fin es la obtención de beneficios económicos o daños a la fama comercial del negocio. Para el profesional de la contaduría pública se ampliará el campo de aplicación, permitiendo estar a la vanguardia de las exigencias del mercado laboral agregando valor a la firma y así ampliar la gama de servicios para ofrecer (auditorías en sistemas).

1.3. Formulación del problema

La problemática causada por la ausencia de directrices para gestionar amenazas y vulnerabilidades que surgen de la interacción con el ciberespacio; plantea la siguiente interrogante: ¿en qué medida afecta la ausencia de procedimientos de gestión de riesgos cibernéticos, que brinden seguridad de la información procesada, manejada y transportada en el ciberespacio; por

las firmas de auditoría y en consecuencia garantizar la confiablidad, integridad y disponibilidad de la misma?

1.4. Delimitación de la investigación

Teórica

La tecnología se ha convertido en una herramienta indispensable para el mundo de los negocios, a tal grado que requiere que empresas como las firmas de auditoría se mantengan a la vanguardia de las innovaciones que esta trae consigo; uno de los avances ha sido la prestación de servicios a nivel del ciberespacio; y firmas de auditoría le apuestan a esta nueva forma de hacer negocios; pero es indispensable tomar en cuenta todos los aspectos que implica apostar a la innovación, ya que no solo consiste en aportar una infraestructura moderna sino también segura. Para tal efecto es necesario, entre otras cosas contar con talento humano capaz de comprender las amenazas, riesgos, retos y oportunidades del ciberespacio.

Según el (BID, 2016) se cuenta con información a través de una serie de informes integrales, preparados y publicados en colaboración con líderes de la industria de seguridad cibernética ofreciendo una imagen más detallada y precisa acerca de la ciberseguridad y delincuencia cibernética en América Latina, además de ello existe normativa técnica y legal que ofrece una guía para la gestión del riesgo, las cuales son: (a) Familia ISO/IEC 27000 - Sistemas de gestión de seguridad de la información emitidas por la Organización Internacional de Normalización, especialmente la ISO/IEC 27032 que trata sobre gestión de riesgo de la ciberseguridad; (b) Marco para la mejora de la seguridad cibernética en infraestructuras criticas emitido por el Instituto Nacional de Estándares y Tecnología; (c) COBIT 5; (d) COSO ERM; (e) Ley Especial Contra los Delitos Informáticos y Conexos; e (f) informes y revistas con referencia a la temática.

Temporal

La investigación se realizó tomando en cuenta el periodo que comprende desde el año 2016 hasta noviembre de 2019, debido a que el 26 de febrero de 2016 se aprobó la Ley Especial Contra los Delitos Informáticos y Conexos en El Salvador, la cual permite regular aquellos delitos que se cometan utilizando las tecnologías de la información.

Espacial o geográfica

La investigación se realizó en una firma de auditoría ubicada en el área metropolitana de San Salvador.

1.5. Justificación del problema

Novedoso

Las TIC a lo largo de la historia han revolucionado el mundo de los negocios, brindando mayores beneficios como minimizar costos, marketing digital, reducción de procesos entre otros. En contraparte ha permitido que terceros interesados utilizando diferentes técnicas de engaño como *phishing*, ingeniería social, *malware*, gusanos, troyanos entre otros obtengan información privilegiada.

En las firmas de auditoría manejan información valiosa de cada uno de los clientes que poseen, dicha información proporcionada a través de diversos medios ya sean físicos o magnéticos corre el riesgo de ser intervenida por terceros no autorizados pues fácilmente podrían disponer de ella obteniendo el dispositivo en donde ha sido resguardada o sustraer físicamente la documentación.

Contemporáneamente los medios para disponer de datos para la realización de los encargos de auditoria se han incrementado a causa de una mayor interacción en el ciberespacio debido a las ventajas que posee; una de ellas es la disposición de la información en el menor tiempo posible y la preservación de grandes volúmenes durante prolongado tiempo.

Es aquí, en donde resulta necesaria la gestión del riesgo del ciberespacio por medio de una guía que proporcione una serie de medidas o controles; que permitan mitigar los riesgos de modo que en caso de sufrir un ataque el impacto sea disminuido. Pues bien, es cierto un riesgo no se eliminará por completo, pero si ayudara a que las pérdidas que se llegaran a desencadenar por el robo de información sean las menores posibles.

Para ello se tomará en cuenta algunos aspectos de la norma ISO 27032 gestión de la ciberseguridad e informes emitidos por organizaciones reconocidas a nivel internacional que brindan las directrices para la gestión del riesgo cibernético

1.6. Factibilidad

Con el surgimiento de la Cuarta Revolución Industrial (nuevas tecnologías que vinculan un mundo tanto físico como digital) la ciberseguridad va retomando mayor relevancia, debido a que las empresas están en mayor contacto con la tecnología y se espera con el tiempo que esto aumente, se tienen ejemplos como el comercio electrónico, pagos electrónicos, por lo cual es necesario que las firmas de auditoría cuenten con medidas para prevenir riesgos de ciberataques como en otros países lo están haciendo.

Considerar que El Salvador no es atractivo para los ciberdelincuentes es un riesgo, por lo cual, aunque no exista un caso reconocido de robo de información, se debe estar consciente que en un momento considerado puede ocurrir pues son riesgos emergentes.

Por eso es importante contar con una guía para la gestión de ataques cibernéticos, que considere los lineamientos establecidos en la ISO 27032, diferentes marcos de referencia en la materia, guías de implementación de otros países como Estados Unidos, Colombia y adecuarlos a la realidad del país; además considerar lo establecido en la Ley especial contra delitos informáticos y conexos.

En El Salvador existen pocos avances en materia de ciberseguridad, cuando hoy en día es factible infectar una computadora con malware existiendo tutoriales incluso para realizar esta acción, esto suena preocupante ya que alguien con conocimientos pocos o muy avanzados, puede ocasionar pérdidas a las firmas de auditoría, "aumenta la superficie sobre las cuales se pueden realizar ataques, proliferan las herramientas para explotar vulnerabilidades y no hay suficientes profesionales preparados para lidiar con estas amenazas" (Fonseca, 2018).

1.7. Utilidad social

La investigación aporta herramientas para la prevención y gestión del riesgo cibernético ante los que están expuestas y vulnerables las firmas de auditoría de El Salvador, con lo que se espera mejorar y garantizar la integridad, confidencialidad y disponibilidad de la información de sus principales activos digitales.

Poniendo en perspectiva esta problemática, se visualizan los beneficios que puede traerle no solamente al sector servicio, sino a los estudiantes y profesionales ya que cualquier individuo que utilice la tecnología es susceptible a un ataque informático, y los delincuentes pueden llegar a obtener información privada.

Por lo cual, es importante dar a conocer medidas para proteger la información personal que tenemos en nuestros dispositivos. Por consiguiente, el profesional de la contaduría pública contará con una herramienta que le ayude a gestionar los riesgos a nivel de ciberseguridad en una entidad atendiendo la demanda de conocimientos que hoy en día exige la profesión respecto a las nuevas tecnologías de la información.

1.8. Objetivos

Objetivo general

Desarrollar una guía de gestión de riesgos cibernéticos que permita prevenir, proteger, detectar, mitigar y responder ante los principales riesgos a los que están expuestas las firmas de auditoría del área metropolitana de San Salvador, El Salvador y generar así un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información.

Objetivos específicos

- Evaluar la situación actual de la gestión de riesgos cibernéticos y los recursos que destinan las firmas de auditoría.
- Identificar los principales riesgos, amenazas y vulnerabilidades a los que está expuesta la información de firmas de auditoría; como resultado de la interacción entre personas, software, conexión de dispositivos y redes.
- Diseñar una herramienta que permita crear un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio para firmas de auditoría.

CAPÍTULO II. MARCO TEORICO

2.1. Antecedentes

Cambios económicos, políticos, educativos, sociales y la naciente necesidad del uso de nuevas herramientas de información y comunicación, son solo algunos aspectos que el mundo ha experimentado. Como respuesta a este entorno, el ser humano ha tenido que buscar soluciones, adaptarse a los cambios o correr el riesgo de estancarse ante un mundo que día a día está cambiando. En este contexto surgen lo que se conoce como las TIC en donde muchos son los avances que en este sentido se han dado y pudieran citarse, algunos ejemplos: (ver figura 1).

Ante lo anterior surge una nueva problemática, ya que las TIC se han vuelto parte importante para los distintos usuarios, inclusive se considera que el acceso a la tecnología y lo que está engloba debería ser reconocido como un derecho humano. Dichas tecnologías traen consigo riesgos, amenazas y vulnerabilidades; por consiguiente, es necesaria la existencia de un marco normativo y legal que permita el control, seguridad y reconocimiento de las mismas.

> A partir de las últimas décadas surgieron nuevas demandas en sectores sociales de diversos países por el derecho al desarrollo, al progreso, a la autodeterminación, a la paz, a un ambiente sano, a la libertad informática, a la identidad (…). Esta generación de derechos viene a responder a nuevas necesidades de la sociedad que no habían aparecido antes y en el contexto de la contaminación de las libertades ante los usos de algunas nuevas tecnologías. (Bailón, 2012, pág. 113)

En este contexto (Digitales, 2018) refiere que uno de los primeros esfuerzos por garantizar la seguridad en el uso de las tecnologías se dio en 1995; en donde los Estados miembros del Consejo de Europa crearon un comité contra delitos informáticos que brindarán alternativas ante la

necesidad de prevenir los actos que pongan en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos.

Teléfono	Se patentó en 1871, su creador Antonio Meucci lo nombró teletrófono 9 de julio de 1877 se fundó la primera compañía de teléfonos. Primer servicio de telefonía comercial, 1946, San Luis EE.UU. Sistema celular: primera descripción nació en 1947 en el trabajo de D.H Ring.
Satélites	En 1960 se lanzó el primer satélite de comunicaciones.
Computadoras	Máquina analítica, finales de la década de los años 40. idea que no se realizó, probablemente por la incapacidad de la tecnología, meramente mecánica, de la época. El matemático inglés George Boole sienta las bases de los que se conoce hoy en día como teoría de la información. Máquina tabuladora de Hollerith, precedente comercial e industrial 1890 Máquina universal de Turing: computador teórico abstracto, 1936. En 1939, un joven ingeniero alemán llamado Konrad Zuse desarrolló el primer computador digital
Internet, red y web.	La semilla de la internet se sembró con la aparición de la red conocida como ARPANET, 1969. *La Word wide web* (conocida como web o www) se creó en 1989; en el laboratorio de física de partículas europeo, Génova Suiza.

Figura 1. Avances tecnológicos relacionados. Rescatado de Breve historia de la informática, 2000. Rescatado de la página web https://s3.amazonaws.com

Uno de los avances tecnológicos viene dado por un mundo que combina lo físico con lo virtual, al cual se le denomina ciberespacio y que trae consigo importantes herramientas y a su vez ventajas y desventajas.

"El término ciber se ha usado para describir casi todo lo que tiene que ver con computadoras y redes y especialmente en el campo de la seguridad" (Caro, 2011, pág. 53). No existe un término general para ciberespacio y puede concebirse de manera distinta, su definición va desde un espacio virtual, interconexión de sistemas en una red u otras definiciones.

Pero conforme el uso de este mundo virtual avanza; nuevos riesgos, amenazas y vulnerabilidades nacen, y es necesario saber que estos van más allá de los riesgos de información o informáticos; y es aquí donde el uso de plataformas, redes inalámbricas, infraestructura requiere de un marco que le permita contar con la gestión y seguridad de la misma.

Es así como en el año 2001 los Estados miembros del consejo de Europa crean el convenio de Budapest también conocido como Convenio sobre la Ciberdelincuencia, donde se buscaba darle solución a esta nueva problemática.

Caso conocido de ataque cibernético a una firma de auditoría

Una de las compañías de consultoría y auditoría consideradas entre las cuatro más importantes del mundo, fue víctima de un ataque cibernético que expuso datos y correos electrónicos confidenciales, algunos de ellos pertenecían a grandes bancos, empresas multinacionales, organismos gubernamentales o, incluso, empresas farmacéuticas. El ataque fue descubierto por la empresa en marzo de 2017 y habría ido directamente y de forma bastante sofisticada contra el servidor global de correo electrónico de la compañía. (guardian, 2017).

En el caso anterior se omite el nombre de la empresa, para efectos de no incurrir en un posible daño a la reputación u otros efectos que pudieran dañar la imagen de la misma.

Situación de las firmas de auditoría

Grandes empresas con reconocimiento internacional de auditoría se han incorporado a las nuevas ideas de negocios, siendo así que incluye en su oferta de servicios diagnóstico y evaluación de la gestión de riesgos cibernéticos, y como bien lo hemos venido explicando estas amenazas cada día les han ocasionado pérdidas millonarias a empresas de gran prestigio; donde sin importar su tamaño están expuestas a casos como robo de información.

En gran medida es importante que antes de poder ofrecer este nuevo servicio las mismas empresas de auditoría se preparen para no sufrir ataques de este tipo, ya que deben comenzar implementándolo internamente, para posteriormente poder aplicarlo a las empresas que contraten sus servicios, puesto que si se ven involucradas en casos como estos perderán prestigio

2.2. Generalidades

Diferencia entre seguridad de la información, seguridad informática y ciberseguridad

Ciberseguridad es un concepto nuevo relacionado a la protección de la información, pero a nivel del ciberespacio por lo que fácilmente se puede confundir con conceptos como seguridad de la información y seguridad informática y hablar indistintamente de ellos. A continuación, se definen cada uno.

Seguridad de la información: la seguridad de la información es aquella que engloba a la seguridad física y a la seguridad lógica compartiendo controles entre sí para brindar protección en donde se localice la información ya sea en papel, usb, discos duros, cd, computadoras y en cualquier forma de resguardo.

Seguridad de la informática: es aquella que está orientada a la mejora de procesos y en general al funcionamiento del sistema informático por medio de la implantación de medidas de protección a la infraestructura tecnológica de las operaciones en la empresa.

Ciberseguridad: es la que se encuentra comprendida dentro de la seguridad lógica y se refiere a la protección de la información que se encuentra almacenada en el ciberespacio por medio de la interacción de personas por medio de dispositivos y los servicios en internet conectados a redes que no tiene existencia física.

Cada uno de los conceptos anteriores están relacionados entre sí y colaboran a la protección de la información sin embargo cada uno lo hace desde un enfoque diferente.

Cuando se refiere a ciberseguridad inevitablemente se puede dejar de mencionar el termino ciberespacio que es aquel que resulta de la interacción entre activos físicos y virtuales cuya existencia no es tangible, en él se llevan a cabo actividades de comunicación, comercio e intercambio.

Las firmas de auditoría hacen uso del ciberespacio para mejorar los servicios que ofrecen a los clientes, debido a las ventajas que supone por lo que esto implica pasar de una seguridad informática o de la información al término de ciberseguridad.

Importancia del ciberespacio

Cuando se emplea el término ciberespacio se visualiza un mundo tecnológicamente avanzado donde la sociedad vive en un entorno virtual separado de la realidad, esto se puede apreciar por ejemplo en la forma de comunicación o de hacer negocios.

Por lo tanto, la existencia del ciberespacio ha tomado trascendencia para todos los usuarios pues facilita una serie de actividades que antes no se podían realizar de manera rápida, por ejemplo, comunicación a larga distancia, envío y recepción de mensajes en tiempo real. Además, por medio de la web se encuentra todo tipo de información y una serie de servicios en línea que diferentes usuarios pueden utilizar como promocionar los productos y servicios por medio de una página web y redes sociales, compras en línea, almacenamiento de información, pagos en línea, utilización de

dinero virtual (bitcoin y criptomonedas), foros de discusión o encontrar todo tipo de información y difundirla.

Cabe destacar que en el ciberespacio se encuentra almacenado un sin fin de información confidencial; por lo que retoma importancia el término de ciberseguridad pues bien es cierto el uso del espacio virtual proporciona enormes ventajas dado que facilita el comercio de productos y servicios permitiendo el acercamiento a los clientes para atender las necesidades y expectativas de cada uno de ellos. Pero paralelo a ello surgen algunas desventajas que de no gestionarlas se podrían convertir en pérdidas grandes para las empresas sin importar el tamaño o clasificación que estas tengan.

Ventajas y limitantes de la ciberseguridad

Ventajas

- Permite preservar la confidencialidad, integridad y disponibilidad de la información.
- Nueva Generación de Auditores

  Auditoria de tecnologías de información nace por la necesidad de conocer los controles e impacto que causa a las organizaciones almacenar los datos contables en sistemas computarizados, (…) no obstante, el tiempo ha transcurrido permitiendo evolucionar las tecnologías con las cuales se gestiona y administra la información. Esto lleva a una evolución digital del auditor de sistemas o de TI, al convertirse en un ciber-auditor que debe conocer los riesgos que implica: la transformación digital, el uso del loT, la nube, entre otros. (Jiménez, 2017)

  Se crean nuevas oportunidades para el profesional en Contaduría Pública, puesto que integra la necesidad de brindar un apoyo técnico a los objetivos estratégicos de una organización, combinando técnicas de auditoria en sistemas, *Ethical Hacking*.

- Brinda un ambiente de seguridad a las cinco entidades del ciberespacio personas, internet, conexión de dispositivos, conexión de redes y software. Permite establecer controles ante las vulnerabilidades y amenazas que pongan en riesgos los activos digitales.
- Permite a las firmas de auditoría proteger la información ante la ciberdelincuencia, ciberguerra, malware, troyanos, gusanos, virus, rootkit, ataques de denegación del servicio e ingeniería social.
- Existen informes por parte de organismos reconocidos que las empresas pueden tomar en cuenta al momento de decidir gestionar los riesgos.
- Fomenta la prosperidad económica para las empresas ya que permite mitigar los posibles riesgos que pueden originarse en el ciberespacio.

Limitaciones

- Destinación de pocos recursos económicos por parte de los empresarios para implantar una gestión de riesgos de ciberseguridad en sus empresas. Debido a que optar por la gestión de riesgos de ciberseguridad implica costos adicionales para la entidad.
- Pocos esfuerzos por parte del gobierno central en invertir en gestión de riesgos del ciberespacio. En consecuencia, la poca o débil regulación de los delitos cibernéticos, limita que se garantice que la información esté segura ante terceras personas.
- Pocas habilidades, competencias y experiencia de los profesionales de una entidad en gestionar riesgos a nivel del ciberespacio.

Ciberseguridad en las firmas de auditoría

La información se está convirtiendo en el activo más valioso con que cuentan las empresas, por esta razón para resguardarla se han utilizado diversas herramientas a lo largo de la historia tales como: impresos en papel, archivos, disquete, CD , DVD, USB entre otros; cada uno de ellos han

contribuido a preservar la información con el paso del tiempo y a mantenerla segura, sin embargo existen nuevas formas de resguardo como el almacenamiento en la nube, que permite disponer de la información en cualquier momento y lugar, además de almacenar grandes cantidades de información.

En las firmas de auditoría se maneja información de gran valor de manera que es indispensable que el equipo de auditoría se comprometa con guardar confidencialidad de toda la información que suministran los clientes. Por este motivo las normas de auditoría de control de calidad resaltan la importancia de contar con un manual de control de calidad que permita que el encargo de auditoría se realice con profesionalismo; incluyendo forma de resguardar la información. Cada miembro integrante del encargo de auditoría debe firmar un acta de confidencialidad, carta compromiso con la firma y verificar conflictos de interés que supongan amenazas para la continuidad con el trabajo de auditoría; por otra parte, cuando se incluye en el negocio las TIC, se incrementan las vulnerabilidades y amenazas, debido a que gran parte de la información se almacenada en el ciberespacio.

Como parte de los trabajos de auditoría las firmas tienen acceso a información privilegiada de sus respectivos clientes, entre las cuales podemos mencionar estados financieros, costos de producción, detalle de gastos e ingresos, inventarios, bienes información tributaria e información personal de los empleados; que pueden ser considerados de valor para terceros interesados en sustraerla para obtener un beneficio (financiero o personal), siendo necesario contar con herramientas, políticas y procedimientos adecuados para proteger información proporcionada.

A medida la tecnología fue evolucionando las firmas de auditoría, se adaptaron a dichos cambios creando páginas web, como una forma de promocionar sus servicios, pero a su vez se debe estar preparados ante las amenazas a las que se verían expuestos.

Como se puede apreciar la información que se maneja a nivel de firmas de auditoría es valiosa por lo que terceras personas con el fin de dañar u obtener lucro económico han encontrado mecanismos para tener acceso a esta sin ninguna autorización de los propietarios, empleado diversas técnicas y aprovechando las vulnerabilidades; estas últimas son las principales causas por las que se pueden dar ciberataques, si la información es divulgada sin autorización puede provocar grandes consecuencias tales como pérdida de confianza (pérdida de clientes).

La información, el activo más valioso con que cuentan las firmas de auditoría se puede ver expuesta por diversos actores que pueden ser (a) internos y (b) externos; los primeros son aquellos que están dentro de la firma y que tiene acceso a información de los clientes, empleados y de la firma misma, los últimos son aquellos que están fuera de la organización pero que buscan obtener información con fines económicos, generar mala reputación y desconfianza; y en general afectar las operaciones de la organización (ver figura 2).

Los actores externos pueden ser ciberdelincuentes, ciber activistas que son los que llevan a cabo ciberataques por razones ideológicas y ciber vandalismo que llevan a cabo las acciones para demostrar sus capacidades.

Otros factores, que suponen riesgos son las vulnerabilidades de los sistemas; pues la mayoría de ataques se dan por que el sistema es débil y con facilidad se obtiene acceso a la información sin la necesidad de emplear métodos sofisticados; están los navegadores *web* que a menudo en las firmas de auditoría utilizan para realizar búsqueda de información acerca del conocimiento del cliente, revisar correos electrónicos, consultar normativa técnica y legal; o promocionar los servicios por medio de una página *web* y redes sociales.

Figura 2. Motivos para desarrollar ciberataques. Rescatado de "ciber amenazas y tendencias 2018" tomado de página web del Centro Criptológico Nacional (España).

Según estudios del Centro Criptológico Nacional de España (CCN, 2018):

Los navegadores de escritorio comúnmente conocidos tienen vulnerabilidades asociadas (ver figura 3) esto debido al uso un sistema de gestión de contenido (CMS) por medio de *plugin* que consisten en aplicaciones que ayudan a otras aportando herramientas de mejora en apariencia, navegación y para la creación de páginas web en otras palabras se puede decir que *plugin* es sinónimo de complemento.

El personal de las firmas de auditoría generalmente navega por sitios web que incorporan publicidad dañina las cuales algunas contienen códigos maliciosos para obtener información y por ende comprometer los datos de los clientes exponiéndolos ante terceros no autorizados.

Otra amenaza que surgen es el *ransomware* consistente en la encriptación de la información de la empresa por parte de un tercero en la que este impide el acceso a la misma solicitando rescate con el fin de obtener ganancia monetaria a corto plazo.

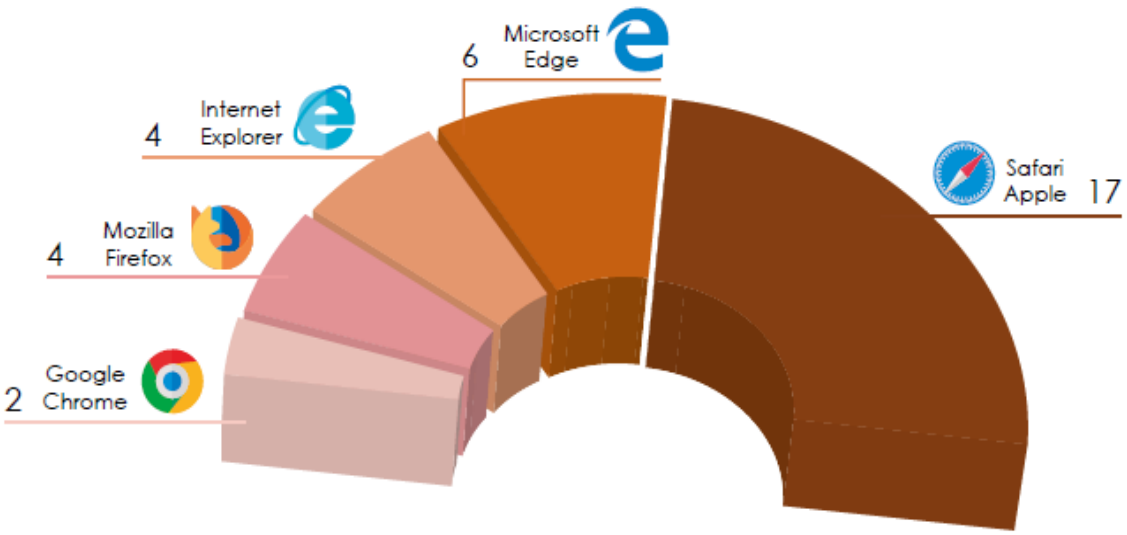


Figura 3. Navegadores web con más vulnerabilidades. Rescatado de ciberamenazas y tendencias 2018. Rescatado de la página web del centro Criptológico nacional (España).

En las firmas de auditoría es necesario tomar importancia a este tipo de eventos pues si bien es cierto no existe un caso reconocido es un riesgo emergente que puede causar enormes retrasos en la prestación de servicios, perdidas de información confidencial, perdidas económicas, de clientes y de empleados. Es necesario que el personal se mantenga informado de las formas de actuar de estos códigos maliciosos pues con el simple hecho de abrir un enlace desconocido o archivos adjuntos a correos electrónicos; no actualizar el antivirus o abrir videos de páginas de dudoso origen se expone la información.

Retos a enfrentar para las firmas de auditoría y el profesional de la contaduría pública

> Big Data, Cloud Computing (la nube), Internet, de las Cosas y Ciberseguridad (...) está produciendo el advenimiento y despliegue de la cuarta revolución industrial. Las sofisticadas amenazas a la propiedad intelectual y a la privacidad, a los sistemas y los productos conectados, requieren estrategias y herramientas de ciberseguridad que garanticen en el marco de la Industria 4.0, ciberseguridad de calidad industrial y habilitados para la tendencia dominante de Internet de las Cosas (Aguilar, 2017, pág. 19).

Como se puede apreciar la ciberseguridad es un elemento clave de la cuarta revolución industrial, la tecnología implica grandes cambios en la idea de negocio de una organización porque proporciona oportunidades de mejora y crecimiento pero al mismo tiempo propicia riesgos, amenazas y actores internos y externos que buscan aprovecharse, en este contexto resulta urgente gestionar tomando en cuenta marcos de referencia y leyes vigentes pues grandes empresas han sido víctimas de incidentes; tal es el caso de Apple:

> En el mes de septiembre de 2015 sufrió el mayor ataque informático de su historia y tuvo que retirar más de cincuenta aplicaciones que contenían un *software* malicioso *(malware)* que pretendía robar datos de los dispositivos de los usuarios. Unos meses antes, Sony Pictures Entertainment quedó paralizada por la intrusión de unos hackers que robaron más de 33.000 documentos con información comprometedora de la compañía y sus empleados (Aguilar, 2017, pág. 21).

Como bien se mencionaba en las páginas anteriores la información que manejan las empresas es valiosa por lo tanto debe estar segura y garantizar la integridad, confidencialidad y disponibilidad de la misma, sucesos como los precedentes suponen una alerta para líderes de las organizaciones o profesionales pues los métodos tradicionales de gestión de riesgo se deben actualizar.

La encuesta global de la federación internacional de contadores (IFAC, 2018) realizada en 150 países, trata acerca de los factores del mercado que probablemente afectaran en el futuro de la profesión de la contaduría pública en la que se hace énfasis en tres aspectos muy importantes: (a) talento humano, (b) tecnología y (c) consultoría. El 54% de las entidades tienen dificultades en atraer talento humano de próxima generación y el 66% de ellos carece de habilidades adecuadas

que supone el mercado tecnológico; esto supone oportunidades para los profesionales en invertir en adquirir nuevas capacidades de acuerdo a la demanda del mercado.

2.3. Base técnica

Sin lugar a dudas cuando se habla sobre ciberseguridad se asocia con la Organización Internacional para la Estandarización (ISO) puesto que: a) proporciona un marco de referencia con alcance internacional; b) engloba la mayor parte de las industrias desde tecnología hasta seguridad alimentaria, agricultura y atención médica; y c) se aplica para productos; servicios y sistemas; gestión de la calidad; seguridad y eficiencia." (Organización Internacional de Normalización, 2019).

Por este motivo se toma de referencia la normativa creada en el año 2012 por miembros del comité técnico "ISO/CEI JTC1/SC27 Seguridad, Ciberseguridad y Protección de la Privacidad"; como medida para afrontar las nuevas amenazas que surgen por la digitalización de la información, y principalmente proporciona una guía para mejorar el estado de la seguridad cibernética, explicando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad" (Organización Internacional de Normalización, 2019).

2.3.1 Norma ISO 27001

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que brinda herramientas de gestión de riesgos de la información, y unos de sus objetivos principales es buscar la confidencialidad, integridad y disponibilidad de los datos. Su base es identificar donde están los riesgos y luego darles un tratamiento.

Gestión de riesgos ISO 27001 y su relación con la gestión del riesgo cibernético.

La gestión de riesgos incluye un conjunto de actividades coordinadas para dirigir y controlar una estrategia en relación al riesgo de una empresa. Incluye por lo general: evaluación de riesgos, tratamiento de riesgos, aceptación y comunicación de riesgos.

A partir de lo anterior, la gestión de riesgos cibernéticos es, aquel conjunto de actividades coordinadas realizadas por una organización con el objetivo de dirigir y controlar la probabilidad de que las amenazas exploten vulnerabilidades de información en el espacio virtual que engloba las TIC.

Por lo tanto, la gestión de riesgos cibernéticos requiere un conocimiento claro de: a) las áreas y actividades que realiza la organización, las características del negocio, sus activos y tecnología; b) un análisis de los riesgos a los que está expuesta la organización; c) las posibles actividades o medidas para el tratamiento de los riesgos; y d) aprobación e implementación de medidas del tratamiento del riesgo.

2.3.2. ISO 27032 GESTIÓN DE LA CIBERSEGURIDAD

La norma facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques, la organización espera que ISO/IEC 27032 permita luchar contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado. (ComputerWord, 2012). Según el grupo Cynthus en su documento denominado “ciberseguridad no es lo mismo que seguridad de la información” la ciberseguridad consiste en brindar a las cinco entidades del ciberespacio es decir ofrecer seguridad a la intersección de personas, internet, conexión de dispositivos, conexión de redes y software.

2.3.3. NTS ISO 31000:2018

La NTS ISO 31000:2018 esta norma es una adopción idéntica (IDT) a la Norma ISO 31000:2018, “Gestión del riesgo – Directrices”; emitida por la Organización Internacional de Normalización (ISO). Esta norma proporciona directrices para gestionar el riesgo al que se

enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto.

Gestión del riesgo y su propósito

El propósito de la gestión del riesgo es la creación y la protección del valor. Mejorar el desempeño, fomentar la innovación y contribuir al logro de los objetivos.

La gestión del riesgo es iterativa y asiste a las organizaciones a establecer sus estrategias, lograr sus objetivos y tomar decisiones informadas.

Compromiso de la gestión del riesgo

La alta dirección y los organismos de supervisión, cuando sea aplicable, deberían articular y demostrar su compromiso continuo con la gestión del riesgo mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de la organización con la gestión del riesgo.

Requerimientos para la gestión del riesgo

Como punto de partida la organización debe establecer: a) el alcance de las actividades de la gestión del riesgo; b) establecer el contexto (entorno) en el cual busca definir y lograr sus objetivos; c) definir los criterios de riesgos que se pueden asumir y cuales no;

Una vez identificados los puntos anteriores es proceder a la valoración del riesgo; la cual incluye de manera global la identificación del riesgo, análisis del riesgo y valoración del riesgo.

Los últimos puntos consisten en a) darle tratamiento al riesgo, seleccionando e implementando opciones para abordar el riesgo; b) el proceso y sus resultados se deberían documentar e informar a través de los mecanismos apropiados y; c) dar seguimiento y revisión con el propósito de mejorar la calidad y eficacia del diseño, la implementación y los resultados obtenidos.

2.3.4. Iniciativas

Por otra parte, se enfatiza que sectores empresariales, gubernamentales con alto reconocimiento internacional, realizan estudios con la intención de concientizar a los consumidores o la población de determinada región. Tal es el caso de una reconocida empresa de telecomunicaciones pública en el año 2016, un documento que retoma aspectos como la protección de la información en un mundo digital, posterior a su publicación la empresa con sede en España se ve afectada por uno de los mayores ataques cibernéticos. A partir de entonces ha incursionado en temas relacionados con la ciberseguridad.

Debido a la creciente interacción de los individuos con las Tecnologías de la Información (especialmente Internet), surgió la preocupante sobre los riesgos a los cuales estaban expuestos, ya que las herramientas que brinda podían ser usadas para el cometimiento de crímenes. Por esta razón, a iniciativa del Consejo de Europa se crea el Convenio de Budapest, que busca proteger tres aspectos fundamentales de los datos informáticos como lo son: confidencialidad, integración y disponibilidad. (Asimismo es importante mencionar que es base fundamental para la creación de la Ley de Delitos Informáticos y Conexos vigente en El Salvador).

El último que se ha firmado es donde varias empresas privadas firman un protocolo de ciberseguridad donde establecen parámetros y líneas de acción encaminadas al mundo actual que vivimos**.**

2.4. Base legal

Con el objeto de brindar una herramienta que permita reducir las amenazas que surgen a medida van evolucionando las tecnologías de la información, los gobiernos centrales a nivel internacional han creado una serie de leyes y reglamentos aplicables en su jurisdicción sobre ciberseguridad. En algunos casos se han formado alianzas estrategias, puesto que se considera necesario ampliar la

protección de cobertura para los usuarios, por el nivel de alcance que tienen los delitos cibernéticos; es decir, un determinado usuario puede estar protegido en su país de origen al existir regulación, pero en ocasiones los ataques cibernéticos pueden originarse en otros países. Por tal motivo los gobiernos se ven interesados en concientizar a otros países sobre los riesgos que existen en el ciberespacio.

La ciberseguridad requiere de normativa tanto nacional como internacional, que permita la regulación del actuar en materia, adicionalmente requiere de profesionales que la apliquen y pongan en manifiesto la ética profesional. Por tal motivo se realiza una comparativa en cuanto a la regulación legal existente en El Salvador sobre ciberseguridad, como primer punto, que, si bien es cierto que existen leyes que permitan disminuir el cometimiento de delitos relacionados/cometidos con las TIC'S, es necesario que se siga promoviendo la implementación de medidas de protección y capacitación sobre el tema. Actualmente se encuentran vigentes en El Salvador las siguientes leyes relacionadas con el tema:

Ley Especial contra los Delitos Informáticos y Conexos

Con el incremento en el uso de medios electrónicos para enviar, recibir o resguardar información; se vuelve prioridad el proteger, prevenir y sancionar aquellos delitos en perjuicio de datos almacenados y sistemas informáticos, cometidos por medio de las TIC, que afecten la identidad, imagen, intimidad o propiedad del afectado, para obtener un beneficio patrimonial, daño o manipulación de la información.

Contextualizando, anteriormente a la entrada en vigencia de la Ley; la legislación penal de El Salvador hacía referencia al cometimiento de los delitos relacionados con las tecnologías de la información, utilizando términos como "por medios electrónicos". Por lo tanto, ante la proliferación de amenazas que vulneran la integridad de la información procesada, almacenada y

transmitida en sistemas tecnológicos; en el año 2016 entra en vigencia la ley especial contra los delitos informáticos y conexos, que facilitara la detección, investigación y sanción de aquellos delitos cometidos por medio de las TIC.

Entre la diversidad de actividades delincuenciales que pueden cometerse a través de las los TIC, que se encuentran reguladas en dicha ley podemos mencionar: a) delitos contra los sistemas tecnológicos de información informáticos; b) delitos informáticos donde se tiene por objetivo la obtención, manipulación o perjuicio de la información, como por ejemplo estafa, fraude, espionaje, técnicas de denegación de servicio; c) delitos informáticos relacionados con el contenido de los datos; y d) delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad.

Delitos informáticos en contra de sistemas tecnológicos de información

Accesos indebidos, interferencia, daños y posesión de equipos o prestación de servicios para la veneración de la seguridad, son riesgos contemplados en el primer capítulo; donde se establece la importancia de proteger los activos de información con que cuentan la empresa, entendiéndose como aquellos relevantes para crear, procesar y almacenar información que permite el buen funcionamiento de la empresa. Ya que a medida se incorporan las TIC a la idea de negocio, se descuida la parte de seguridad de la información, aumentando las probabilidades de ataques cibernéticos.

En este capítulo se separa dos aspectos importantes que son el daño causado al bien en particular como son los sistemas informáticos, alterando su buen funcionamiento; y en contra parte tenemos accesos indebidos intencionalmente o no por parte de terceros interesados en obtener un beneficio económico ejemplo de ellos pueden llegar a ser incluso empleados de la misma compañía: (ver figura 4).

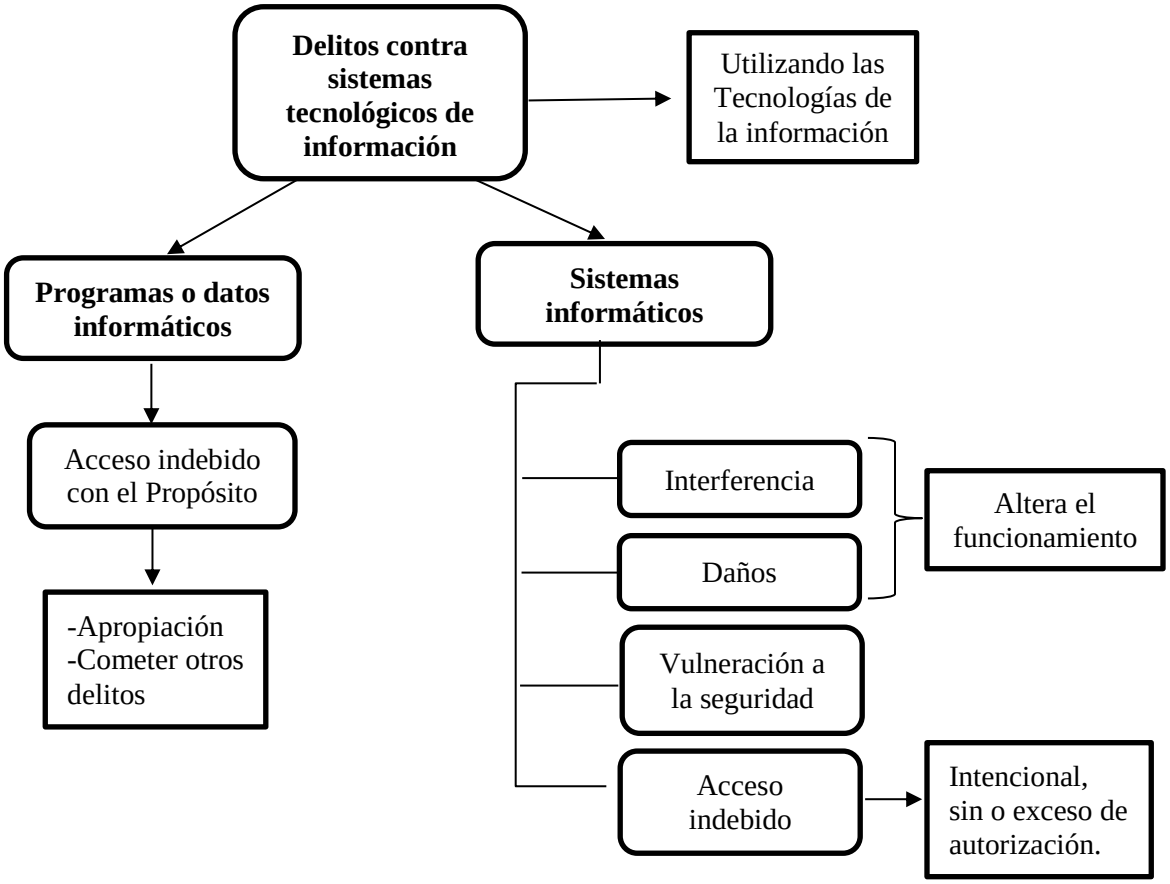


Figura 4. Delitos cometidos contra sistemas tecnológicos de información. Se detalla aquellos delitos cometidos contra sistemas tecnológicos de información regulados por la ley especial contra delitos informáticos y conexos. Rescatado de página web Asamblea Legislativa de El Salvador.

Delitos informáticos

Estafa, fraude y espionaje informático, por mencionar algunos; atentan contra el patrimonio o de contenido patrimonial donde traerá consigo una relación de al menos dos personas, por una parte, el afectado y el que engaña.

Delitos relacionados con el contenido de los datos

Este se divide en tres secciones importantes: a) manipulación de registros, alteración de información contenida en un registro de acceso; b) alteración, daño a la integridad de los datos: y c) interferencia de datos. (ver figura 5)

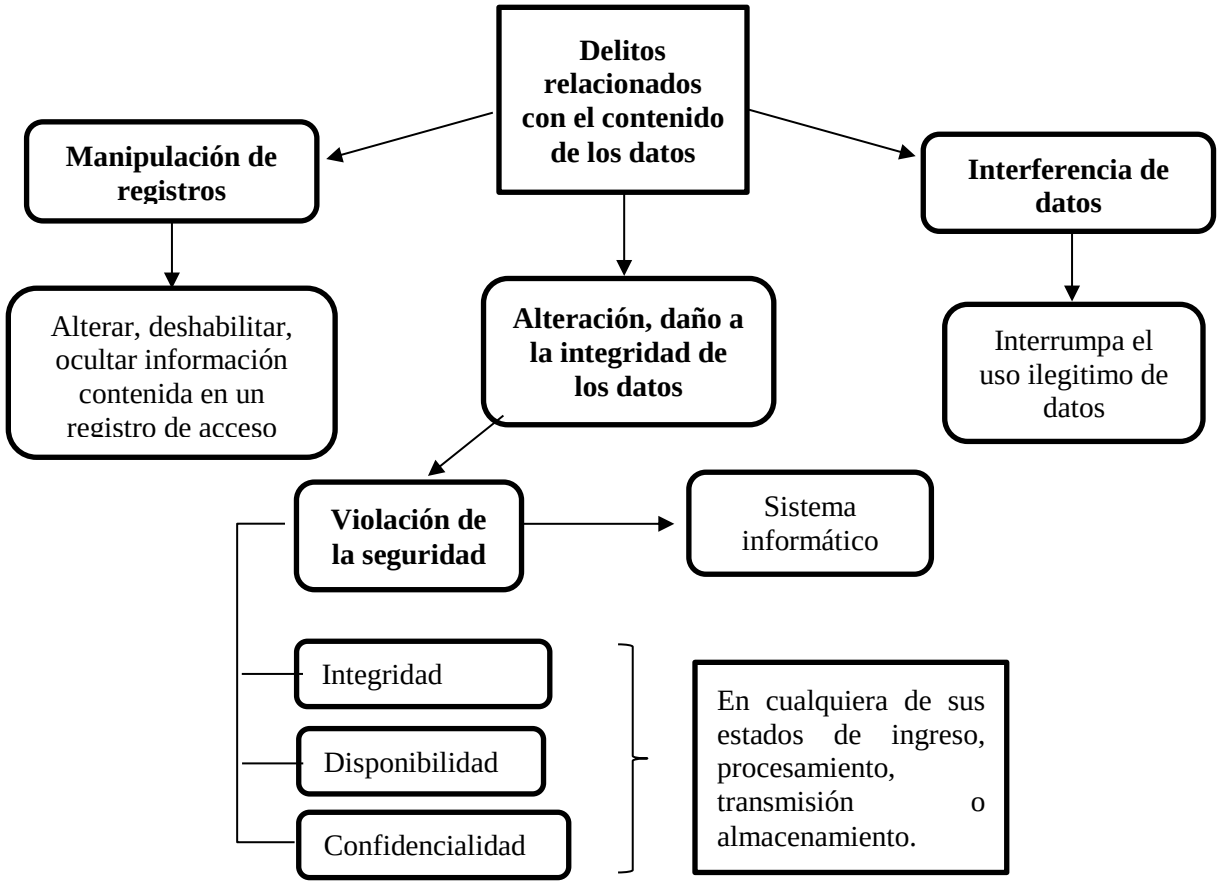


Figura 5. Delitos cometidos, relacionados con el contenido de los datos. Con base en Figura 6 se detalla aquellos delitos que manipulan, alteran, o dañan la integridad de los datos, regulados por la ley especial contra delitos informáticos y conexos. Rescatado de página web Asamblea Legislativa de El Salvador.

Ley de Firma Electrónica

Esta Ley fue aprobada en el año 2015 y entra en vigencia desde abril de 2016, su finalidad es implementar el uso de la firma electrónica, contando con la misma validez jurídica que una firma

autógrafa. En efecto desde su creación se planteaba los múltiples beneficios que traería para la automatización de trámites, sobre todo aumentar la eficiencia y eficacia en los procesos entre las empresas, la ciudadanía y el Estado.

Uno de los mayores desafíos que planteaba en el ámbito de aprobación de la Ley, era crear un clima de confianza entre los usuarios, dado que se utilizara en la medida que se utiliza se tenga una certeza jurídica; por otra parte, el reto consiste en garantizar su implementación.

"El uso de la firma electrónica trae consigo un gran desafío, que consiste en la protección de datos personales. La firma en si es un dato personal, y requiere de mecanismos de protección reforzada" (Calderón, 2017).

En abril del año 2017 se implementó la disposición por parte del Ministerio de Hacienda de presentar a través del Portal web, el formulario Carta de Presentación del Dictamen e Informe Fiscal (F-455), y el Dictamen e Informe Fiscal, los Estados Financieros, las conciliaciones tributarias entre otros. Este mecanismo permite la aplicación de la firma electrónica.

Con respecto a la relación de los principios fundamentales para garantizar la seguridad de la información, con la ley especial contra delitos informáticos y conexos; se encuentra la integridad donde se garantiza que la información en su transmisión no ha sufrido modificaciones o alteraciones hacia su receptor, que se asocia al riesgo cibernético de manipulación de la información por los ciberdelincuentes; en cuanto a la confidencialidad que solo las personas autorizadas podrán descifrar la información que es transmitida.

En el marco para la mejora de la seguridad cibernética e infraestructuras críticas describe que la Gestión de riesgos es el proceso continuo de identificación, evaluación y respuesta al riesgo.

Para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Con esta información, las organizaciones pueden determinar el nivel

aceptable de riesgo para lograr sus objetivos organizaciones y puede expresar esto como su tolerancia al riesgo. Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de seguridad cibernética, para permitir tomar decisiones informadas sobre los gastos de seguridad cibernética. (Instituto Nacional de Estándares y Tecnología, 2018, 4).

Ley de Propiedad Intelectual

El Art. 32 de la presente ley regula la protección de programas de ordenador, código fuente o programa objeto debido a que se consideran obras literarias. Se permite la reproducción lícita sin autorización del autor de una copia del software cuando sea para fines de respaldo o seguridad, para el uso del personal del usuario, con la condición que no atente contra los derechos normales del autor de la obra.

Se debe considerar que: "no constituye una modificación de la obra, la adaptación de un programa de ordenador realizada por el propio usuario y para su utilización exclusiva" (Art.49, página 13 Ley de Propiedad Intelectual). Cuando se cuente con una previa autorización del propietario, se realicen pruebas, correcciones, o investigación sobre la seguridad de una computadora; constituye una excepción a la prohibición regulada en el Art. 85-D inciso 2 literal; siempre y cuando no afecten la adecuada protección legal contra la evasión de medidas tecnológicas, entendiéndose como cualquier tecnología que controla el acceso a una obra, o que proteja cualquier derecho de autor.

El plazo de la protección de acuerdo al Art. 86 para el software, si es una persona natural el propietario comprende la vida de este y cincuenta años adicionales contados a partir del día de su muerte a favor de los herederos. En caso se tratase de una persona jurídica, son 50 años, contados a partir del primero de enero del año siguiente al de la primera divulgación autorizada.

CAPÍTULO III. DISEÑO METODOLÓGICO

3.1 Tipo de estudio

Al analizar la naturaleza del problema y sus objetivos, se determinó que la investigación debe abordarse bajo el enfoque cualitativo el cual requiere un proceso inductivo, interpretativo, interactivo y recurrente; apropiado para el estudio de las problemáticas que han sido poco exploradas.

3.2. Unidades de análisis

Las unidades de análisis para esta investigación son las firmas de auditoría cuyas oficinas están ubicadas en el área metropolitana de San Salvador.

3.3. Universo y muestra

Universo

Con base en la consideración de los siguientes aspectos: (a) capacidad operativa de recolección y análisis; (b) entendimiento del fenómeno y (c) la naturaleza del fenómeno en análisis, se determinó que el universo de la problemática abordada está conformado por firmas de auditoría que incorporen en su idea de negocio las tecnologías de información y comunicación por medio de la interacción en el ciberespacio y por encargados del departamento de informática, auditoría y expertos.

Muestra

Debido al tipo y objetivo de la investigación no se requiere de una muestra.

3.4. Instrumentos y técnicas a utilizar en la investigación

Técnicas de recolección de datos

Se utilizó la entrevista como medio de recolección de información, la cual se le realizó al Gerente de Informática de una firma de auditoría del área metropolitana de San Salvador.

Instrumentos

El instrumento utilizado fue un cuestionario prediseñado del contenido de la entrevista, con la finalidad de conocer la situación actual de la firma de auditoría respecto al uso del ciberespacio y las medidas de protección de la información. Así mismo se utilizaron anotaciones o notas de campo y textos susceptibles a cambios en cualquier etapa del estudio. Ver anexo 3

3.5. Procesamiento de la información

Posterior a la implementación de los instrumentos y técnicas de investigación el procesamiento de la información fue el siguiente: a) captura, transcripción y orden de la información a un formato legible; b) codificación de la información; a través de la agrupación de información obtenida en categorías que concentran ideas, conceptos o temas; c) obtención de subcategorías; y d) definición de categorías.

El procesamiento se realizó con la ayuda del software Atlas.ti que consiste en un potente conjunto de herramientas para el análisis cualitativo de grandes cuerpos de datos textuales, gráficos y de vídeo. La sofisticación de las herramientas permite organizar, reagrupar y gestionar material de manera creativa y, al mismo tiempo, sistemática. Ver anexo 4

3.6. Análisis e interpretación de los datos procesados

Procesada la información, se integró la información (se utilizó el software Atlas.ti 8) relacionando las categorías encontradas y los códigos correspondientes, con el objetivo de obtener la realidad amplia del problema y elaborar conclusiones a partir de las explicaciones. Ver anexo 5.

3.7. Diagnóstico de la investigación

La gestión de riesgos cibernéticos, es aquel conjunto de actividades coordinadas realizadas por una organización con el objetivo de dirigir y controlar la probabilidad de que las amenazas exploten vulnerabilidades de información en el espacio virtual que engloba las TIC.

Con el objetivo de conocer la situación de las firmas de auditoría respecto al uso del ciberespacio y las medidas de protección de la información se realizó una entrevista que se enfocó en cuatro aspectos importantes los cuales son: a) conocimiento de la firma de auditoría; b) tecnologías de la información y comunicación; c) medidas de control interno; y d) uso de recursos técnicos.

A partir de lo anterior se determinó que:

Los esfuerzos de ciberseguridad han aumentado a partir de la creación de leyes, marcos técnicos y medidas de seguridad cibernética desde el departamento de informática con la creación de unidades de ciberseguridad. Generando oportunidades para el profesional de la contaduría pública como responsables de la gestión del riesgo cibernético para las firmas de auditoría. (ver figura 9)

Es evidente que el ciberespacio trae consigo oportunidades y ventajas para el mundo de los negocios, pero, de la misma forma trae consigo riesgos; a tal grado que existen casos de empresas que han sido víctimas de ciber atacantes. Estos, ocupan técnicas de ingeniería social, *hacking*, *malware* y otra serie de ciberataques aprovechándose de las vulnerabilidades del negocio. (ver figura 10).

En un entorno que apunta cada vez más a la digitalización y al uso de un nuevo mundo virtual (ciberespacio), nadie está completamente exento de ser víctima de un ciberataque y las empresas no son la excepción (para el caso las firmas de auditoría); sin importar el sector económico al que pertenezcan; a tal punto, que el impacto de un ciberataque sobre el negocio puede traer consigo repercusiones como: a) interrupciones de servicios ofrecidos; b) daños reputacionales, problemas jurídicos y financieros; c) pérdida de clientes; e d) incluso provocar la quiebra del negocio. (Ver figura 13 y 14).

Del mismo modo, es de resaltar que cada día aumenta el número de ciber atacantes y los ataques son más innovadores. Por lo tanto, cada uno de los actores involucrados y responsables de la gestión del riesgo cibernético (ver figura 11 y 18) debe asumir su responsabilidad y cumplir su rol, para sobreponerse ante estas situaciones, eliminando todo tipo de limitante y buscar las mejores oportunidades para el negocio. (Ver figura 16).

3.8. Formulación de hipótesis

Hipótesis de trabajo

El diseño y posterior implementación de una guía de gestión de riesgos cibernéticos, contribuirá a mejorar la seguridad de la información contenida y manejada en el ciberespacio; y a garantizar la confiablidad, integridad y disponibilidad de la misma en las firmas de auditoría.

Determinación de variables

- **Variable independiente:**

Guía de gestión de riesgos cibernéticos.

- **Variable dependiente:**

Mejorar la seguridad de la información contenida y manejada en el ciberespacio y a garantizar la confiablidad, integridad y disponibilidad de la misma en las firmas de auditoría en el área metropolitana de San Salvador.

Operacionalización de variables.

Tabla 1. Operacionalización de variables.

Formulación del problema	Objetivo general	Hipótesis de trabajo
¿En qué medida afecta la ausencia de procedimientos de gestión de riesgos cibernéticos, para contribuir a la seguridad de la información contenida y manejada en el ciberespacio por las firmas de auditoría y en consecuencia garantizar la confiablidad, integridad y disponibilidad de la misma?	Desarrollar una guía de gestión de riesgos cibernéticos que permita prevenir, proteger, detectar, mitigar y responder ante los principales riesgos a los que están expuestas las firmas de auditoría del área metropolitana de San Salvador, El Salvador y generar así un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información.	El diseño y posterior implementación de una guía de gestión de riesgos cibernéticos, contribuirá a mejorar la seguridad de la información contenida y manejada en el ciberespacio; y a garantizar la confiablidad, integridad y disponibilidad de la misma en las firmas de auditoría.

Fuente: Autoría propia

Variables	Medición de las variables
Variable independiente: Guía de gestión de riesgos cibernéticos.	• Factibilidad de aplicación de procedimientos de gestión de riesgos cibernéticos • Conocimiento de leyes y normativa aplicable • Disponibilidad de la administración para la aplicación de la guía de gestión de riesgos cibernéticos • Nivel de riesgo aceptado por la administración.
Variable dependiente: Mejorar la seguridad de la información contenida y manejada en el ciberespacio y a garantizar la confiablidad, integridad y disponibilidad de la información en las firmas de auditoría en el área metropolitana de San Salvador.	• Niveles de seguridad alcanzados • Disminución de riesgos • Información confidencial, integra y disponible.

Fuente: Autoría propia

3.9.Cronograma de actividades

MESES / SEMANA	Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ACTIVIDADES																																
PLANIFICACIÓN DE LA INVESTIGACIÓN																																
Planteamiento del problema																																
Delimitación del problema																																
Justificación de la investigación																																
Objetivos de la investigación																																
Diseño metodológico																																
Formulación de Hipótesis																																
Entrega de anteproyecto																																
CAPÍTULO I PLANTEAMIENTO DEL PROBLEMA																																
CAPÍTULO II MARCO TEÓRICO																																
Marco teórico																																
CAPÍTULO III DISEÑO METODOLÓGICO																																
Elaboración de entrevistas																																
Recolección de información																																
Procesamiento de información																																
Análisis de la información																																
CAPITULO IV PROPUESTA DE INVESTIGACIÓN																																
Elaboración de la propuesta																																
Entrega de propuesta																																
CONCLUSIONES Y RECOMENDACIONES																																
Revisiones																																
Entrega de trabajo final																																
Defensa de trabajo de graduación																																

3.10. Presupuesto de costos a incurrir

Tabla 2.

Presupuesto de costos a incurrir de marzo a octubre 2019

Tipo de gasto	Detalle de gasto	Sub total	Total
Gastos directos			**$ 290.00**
Papelería / impresiones	Papel bond/ de avances otros documentos necesarios.	$ 220.00	
Fotocopias	Libros, folletos, bitácoras de asesorías	$ 5.00	
Anillados y empastados	Avances y documento final	$ 30.00	
Utilería	Lapiceros, folder, fasteners, otros	$ 5.00	
Depreciación de equipos	Uso de computadoras	$ 30.00	
Gastos indirectos			**$ 880.00**
Servicio de internet	Mensualmente $ 40.00	$ 320.00	
Servicio de energía eléctrica	Mensualmente $ 10.00	$ 80.00	
Transporte	Pasajes	$ 480.00	
Otros gastos			**$ 320.00**
Alimentación	Reuniones	$ 320.00	
Total de inversión			**$ 1,490.00**

Fuente: Autoría propia

CAPÍTULO IV. GUÍA DE GESIÓN DE RIESGOS CIBERNÉTICOS PARA EMPRESAS DEDICADAS A BRINDAR SERVICIOS DE AUDITORIA EXTERNA

4.1. Planteamiento del caso

La propuesta de solución tiene como finalidad sugerir lineamientos y controles claves que puedan implementarse; de igual modo permite crear un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Cada organización que implemente la guia de gestion de riesgos, ajustara las disposiciones contenidas, de acuerdo con los recursos economicos que disponga.

4.2 Estructura de la propuesta

El diseño de la Guía de Gestión de Riesgos Cibernéticos se encarga de proteger los datos y sistemas críticos de las firmas de auditoría; se compone de cuatro fases que se describen a continuación:

Fase 1. Diagnóstico y evaluación de la organización: en esta fase se realiza una investigación para conocer sobre los procesos, servicios y productos que tiene la organización para determinar su relación con el ciberespacio; con la finalidad de identificar los elementos que deben ser protegidos y permite la creación de medidas de control de ciberseguridad adecuados para la organización, a la regulación legal aplicable.

Entre los aspectos importantes a revisar se encuentran: marco normativo de seguridad aplicado, medidas de seguridad implementadas e identificar los principales activos digitales de la organización incluidos personal.

Fase 2. Análisis de riesgos ciberneticos: en esta fase se retoma la información recopilada anteriormente para identificar las principales amenazas, vulnerabilidades que pueden poner en peligro los activos digitales de la organización, como resultado de la interacción con el

ciberespacio; Se debe considerar el impacto que podría ocasionar la materialización de un evento crítico.

Por otra parte se deben considerar: (a) el tipo y alcance del daño, entre los cuales podemos mencionar virus informáticos, robo o manipulación de la información por terceros interesados *(hackers)* o empleados mal intencionados; (b) lineamientos descritos en normativa técnica y legal vigente. Donde se obtendrá como resultado medidas de control de seguridad basadas en la gestión de riesgos cibernéticos que están orientadas en las necesidades de las firmas de auditoría.

Fase 3. Plan de acción: al obtener conocimiento de los riesgos que pueden afectar a corto o medio plazo a la firma de auditoria, se realiza el plan de acción personalizado, adecuado a las prioridades, amenazas detectadas, tamaño de la empresa, numero de personal, y los lineamientos normativos descritos en informes de ciberseguridad.

En definitiva para que la gestión de riesgos de resultados efectivos, las firmas de auditoría deben tomar implementar medidas adicionales como se detallan a continuación:

- Identificación de roles y responsabilidades a personal clave. Se le asignan tareas específicas que facilitarán la implementar ante las nuevas medidas de protección descritas en la guía de gestión.
- Políticas de protección de ciberseguridad que permitan disminuir, mitigar o reducir el impacto ocasionado en los procesos afectados. Razón por la cual el personal de la firma debe estar capacitado para implementar las nuevas medidas y concientizarlos sobre las consecuencias de las vulnerabilidades de seguridad pueden ocasionar a la firma de auditoría.

Fase 4. Implementación: en esta fase se materializarán los procedimientos establecidos en la guía de gestión de riesgos cibernéticos, considerando adicionalmente que deben estar en constantes actualizaciones de acuerdo a las nuevas amenazas que puedan surgir.

En esta fase también se desarrollará un *check list* para el manejo de incidentes en ciberseguridad, con la finalidad de mostrar las actividades a considerar dentro del control interno para evaluar las acciones a seguir antes, durante y después de un incidente en seguridad. (Ver figura 8).

4.3 Beneficios y limitantes de la guía.

Beneficios:

- Protección de la información a nivel de ciberespacio, mediante la implementación de una serie de medidas que define la guía.
- Al implementar la guía se reducirá el riesgo de un ataque cibernético, por lo que se evitará incurrir en gastos adicionales que implique el desarrollo del incidente.
- Proteger el prestigio e imagen la firma de auditoría y en caso que se desarrolle un incidente, reducir la duración e impacto.
- Reducir la posibilidad de incurrir en demandas jurídicas por robo de información de los clientes.
- Incluir el riesgo cibernético como parte de la gestión estratégica de la firma de auditoría, permitiendo que se esté en constante evaluación del entorno, promoviendo estrategias de mejora.

Limitantes

- Los socios de la firma de auditoría, dispongan poco o nada de esfuerzos y recursos necesarios para la implementación de la guía de gestión.

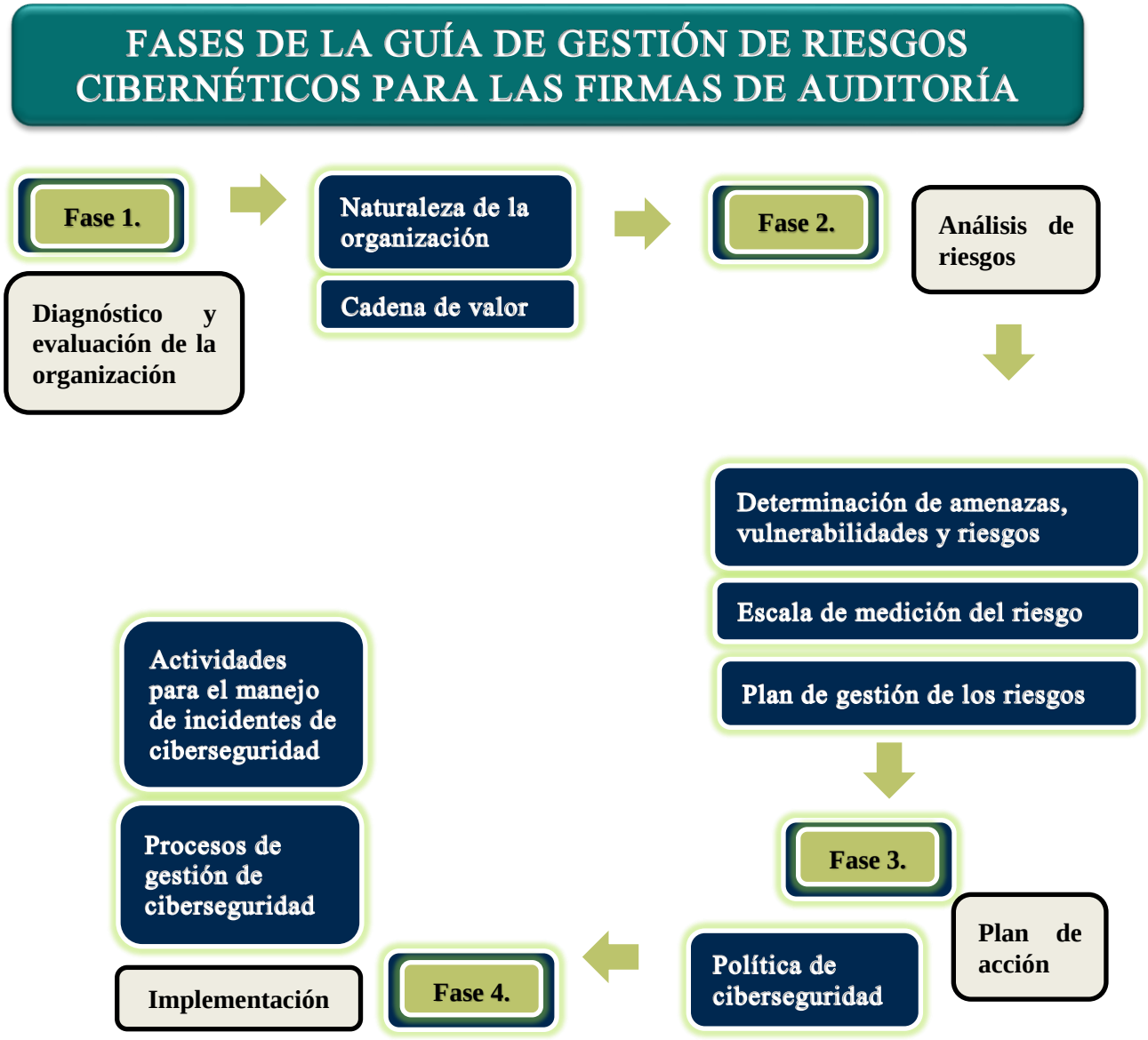


Figura 6. Estructura del plan de solución. Autoría Propia

AGR Auditores
CRECIENDO CONJUNTAMETE

GUÍA DE GESTIÓN DE RIESGOS CIBERNÉTICOS

ARG AUDITORES, S.A. DE C.V.

2019

Objetivo de la guía

Brindar una herramienta que contribuya a la gestión de riesgos cibernéticos para empresas dedicadas a brindar servicios de auditoría externa; que contenga lineamientos, controles y procedimientos para dar una respuesta inmediata ante un incidente de ciberseguridad.

Finalidad de la guía

La Guía de gestión de riesgos cibernéticos para empresas dedicadas a brindar servicios de auditoria externa, tiene como finalidad implementar lineamientos y controles claves, que mejore el ambiente de seguridad frente a daños que atente contra la confidencialidad y disponibilidad de la información transmitida en el ciberespacio.

FASE 1. DIAGNÓSTICO Y EVALUACIÓN DE LA ORGANIZACIÓN

AGR Auditores CRECIENDO CONJUNTAMETE	**Nombre de la empresa:** AGR, S.A. DE C.V.	**Dirección:** Col. Las Victorias Av. Los Ángeles #1200, Departamento de San Salvador.

Finalidad social: Prestación de servicios de auditoría, contabilidad, consultoría e informática.

1.1 Naturaleza de la organización

AGR auditores es una organización multidisciplinaria con sede en San Salvador, El Salvador; constituida bajo los requerimientos establecidos en el Código de Comercio de El Salvador e inscrita en el registro de sociedades el 10 de enero de 2015, inscrita al N° 63 del Libro N° XIV con fecha 11 septiembre de 2012.

Cuenta con experiencia en servicios de auditoría, contabilidad, consultoría e informática a empresas privadas, bajo la normativa internacional vigente y adoptada por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

1.2 Identificación de objetivos estratégicos, visión y misión

Misión	Visión	Objetivos estratégicos
"Ofrecer a nuestros clientes externos e internos un servicio de calidad basado en la experiencia laboral y profesionalismo de cada uno de los socios que la integran"	"Ser una firma líder en la prestación de servicios profesionales en el mercado nacional e internacional, comprometidos con el cliente, manteniendo un equipo profesional capacitado y cumpliendo con las disposiciones legales.	• Ofrecer servicios de calidad, ser honestos, generar recordatorio de la marca a los clientes. • Consolidarse en el mercado salvadoreño. • Innovar tecnológicamente y potenciar eficiencia, oportunidad y calidad.

1.3 Estructura organizacional

La estructura organizacional de AGR auditores, se muestra en la figura 7.

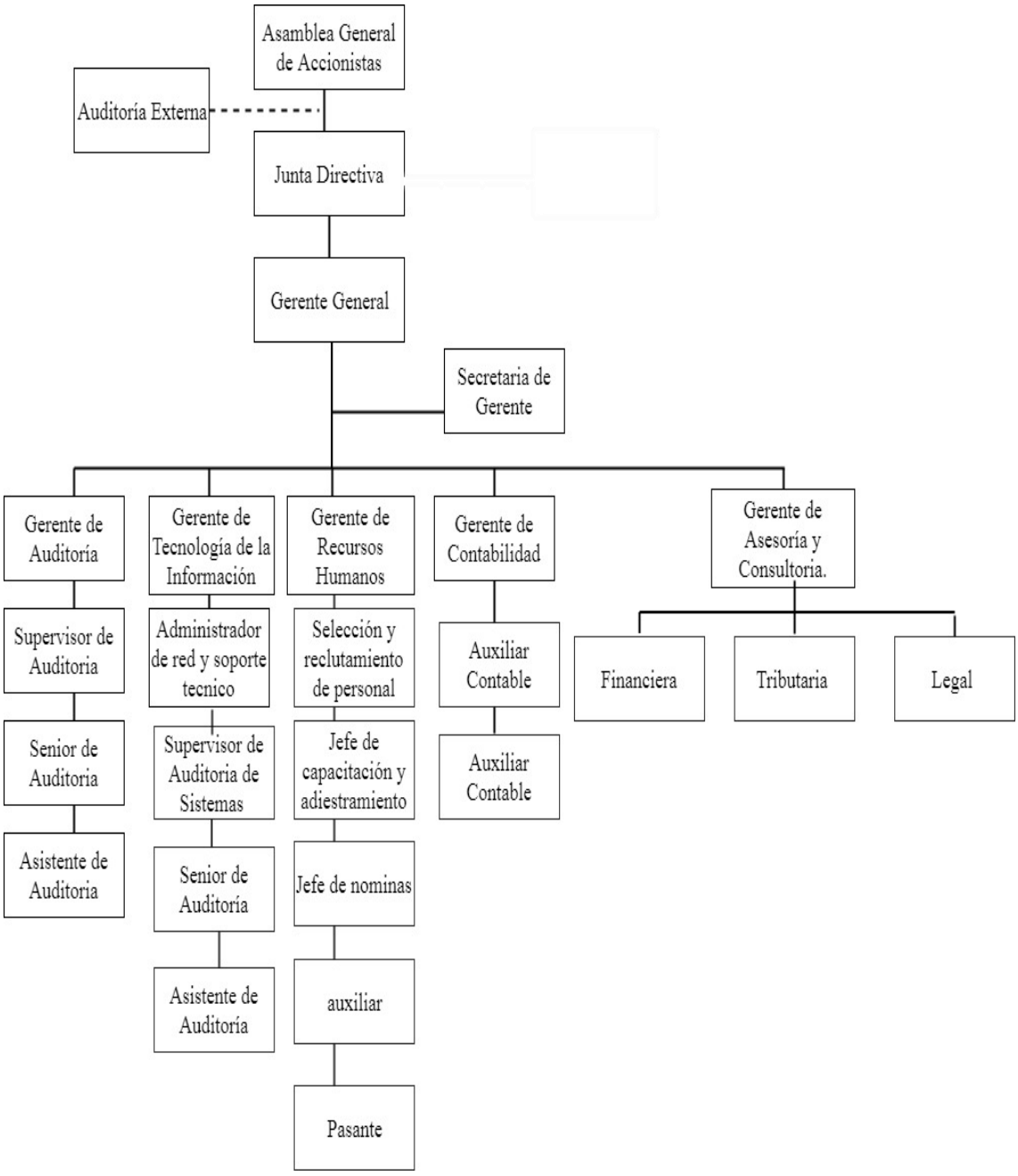


Figura 7. Estructura organizacional propuesta de AGR auditores. Elaboración de una empresa real dedicada a la prestación de servicios de auditoría, contabilidad, consultoría e informática.

1.4 Cadena de valor

La cadena de valor como gestión de riesgos, permite realizar un análisis interno de la empresa AGR auditores, a través de la desagregación de sus principales actividades generadoras de valor. De esta manera identificaremos preliminarmente las necesidades del negocio, recursos que dispone; como se describen en la figura 8.

Hay que mencionar, además que luego de obtener las principales actividades generadoras de valor dentro de la organización, se dividen en misionales y de apoyo como se describen en la figura 8. Es así que las cadenas de valor misional describen la razón de ser de la entidad (fuente de ingresos), por otro lado las de apoyo integra las áreas que son necesarias para el buen funcionamiento de la entidad, aunque no tengan relación directa con la finalidad; y además de factores externos que pueden afectar.

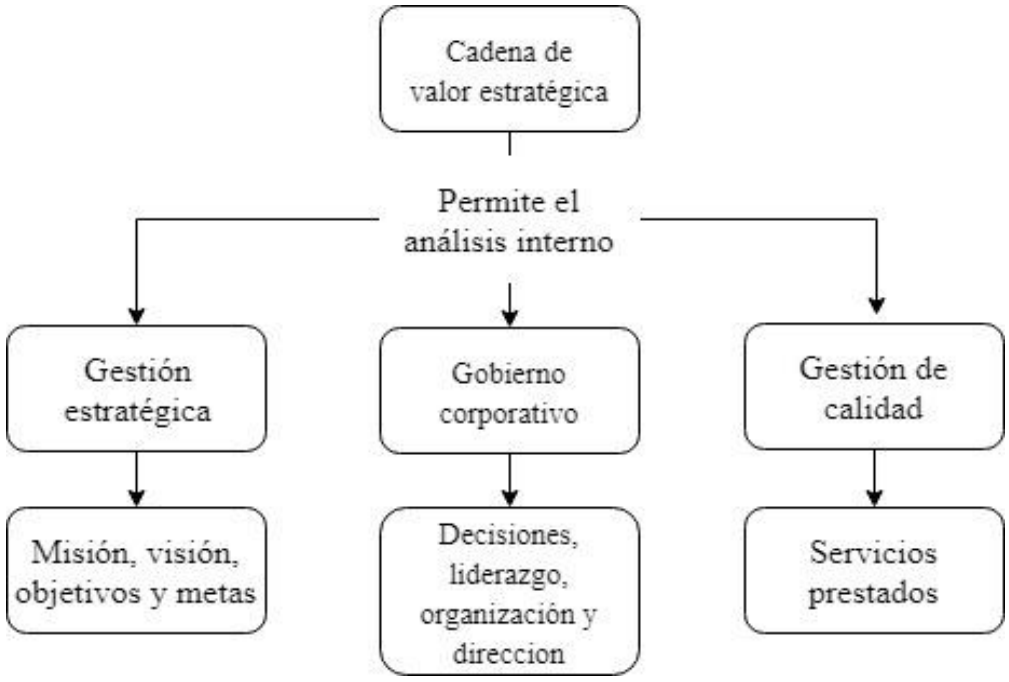


Figura 8. Cadena de valor estratégica. Elaboración propia.

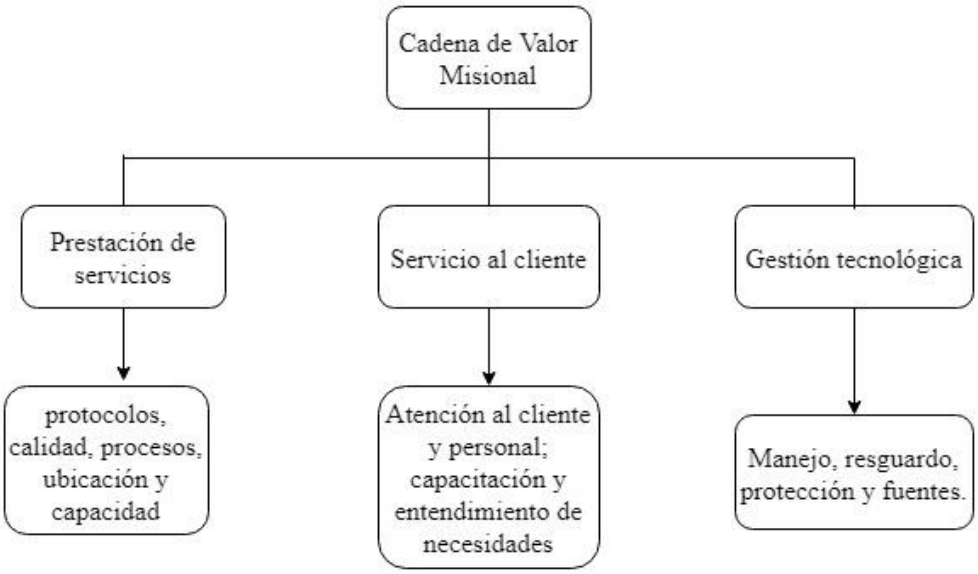


Figura 9. Cadena de valor misional. Elaboración propia.

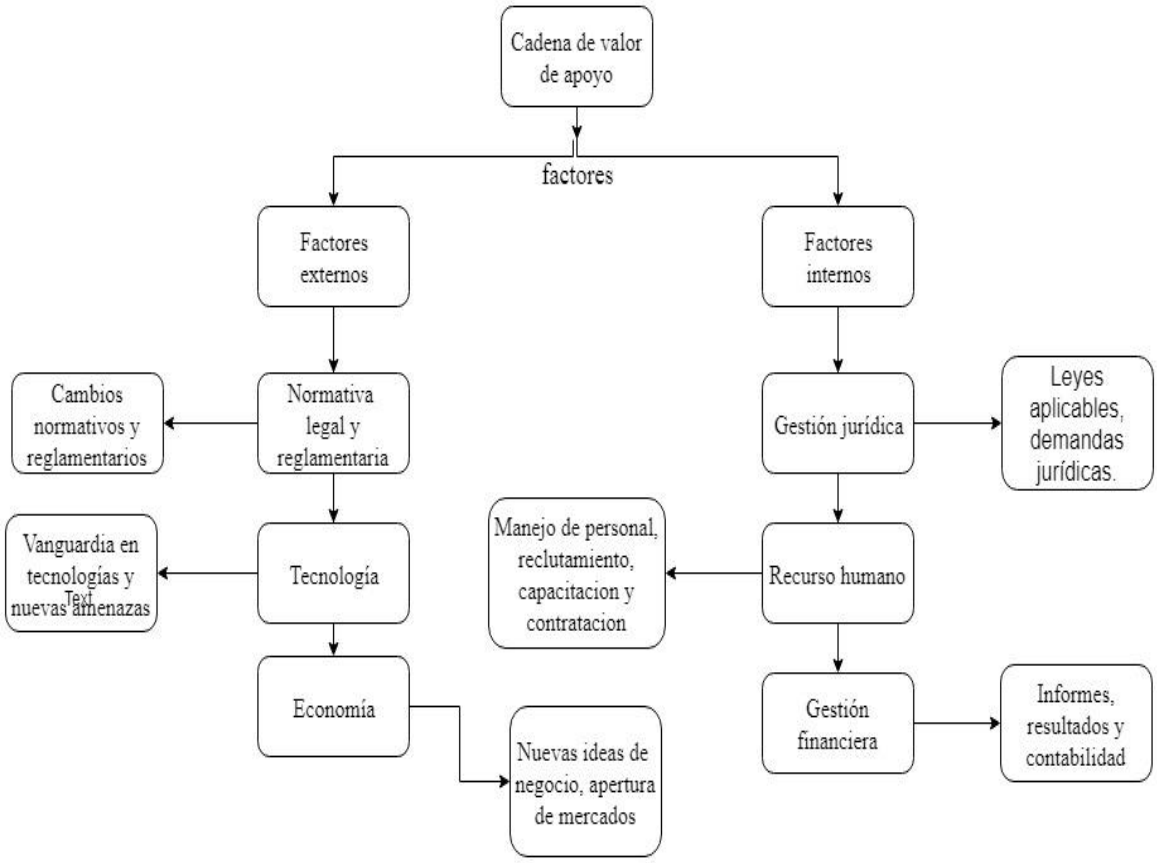


Figura 10. Cadena de valor de apoyo factores internos y externos. Elaboración propia.

1.5 TIC y ciberespacio; medidas de control interno

Uno de los aspectos importantes y necesarios para su análisis es conocer las posibles medidas de control interno que una organización dispone para salvaguardar sus recursos, verificar exactitud de procesos, mejorar la organización y cumplir con sus objetivos.

Para el caso de AGR Auditores las medidas tomadas se muestran en el anexo 3. De acuerdo a lo anterior las áreas con factores de riesgos potenciales en relación con las TIC y ciberseguridad se presentarán de acuerdo al grado de prioridad determinándose las siguientes: gestión de tecnología, recursos humanos y gobierno corporativo.

FASE 2. ANÁLISIS DE RIESGOS CIBERNÉTICOS

2.1 Determinación de amenazas y vulnerabilidades

Con el objetivo de determinar los factores de riesgos internos y externos, con la gestión de la ciberseguridad, se identifican las principales amenazas y vulnerabilidades ligadas al proceso. Se recomienda realizar este procedimiento por lo menos una vez al año, para evaluar los resultados determinados en años anteriores, con el propósito de mantener actualizados los procedimientos y controles actualizados ante posibles amenazas. (Ver tabla 3)

Tabla 3.

Amenazas y vulnerabilidades cibernéticas.

Amenazas	Vulnerabilidades
• Acceso no autorizado a las bases de datos de la empresa, por terceros interesados con fines fraudulentos • Manipulación del sistema a través de *exploit kit* (secuencia de códigos o comando), local o por medios remotos (internet o red). • Fuga de información sensible de la organización.	• Falta de una política de permisos, privilegios y/o control de acceso; fallos en la protección y gestión de permisos. • Ausencia de antivirus adecuados, nula capacitación del personal sobre riesgos cibernéticos. • Ausencia de parches de protección, programas, sistemas y aplicaciones desactualizados; debilidades en el navegador.

Amenazas	Vulnerabilidades
• Ataques por medio de *malware,* a través del uso de *phishing*, permitiendo acceso remoto a un punto final.	• Infraestructura no adecuada, el ancho de banda es menor que el del atacante.
• Denegación de servicio o DoS (*Denial of Service*, por sus siglas en inglés) y la denegación de servicio distribuido o DDoS (*Destributed Denial of Service*).	• Error de configuración**:** Problema de configuración de software o de los servidores web. Provoca la inutilización de páginas web a través de ataques de denegación de servicio (DoS).
• Estafas de correo electrónico o comunicaciones a través de *spear phishing*.	• Ausencia de políticas contra ingeniería social y control de acceso, capacitación al personal.
• Acceso a datos y/o sistemas de control por medio de dispositivos inteligentes.	• Fallo en la validación de datos introducidos en aplicaciones que puede ser una vía de acceso de un ataque.
• Aprovechamiento por parte del atacante, de la escasa legislación en El Salvador aquellos delitos cometidos por medio de las TIC.	• Dificultades legales para la persecución del cometimiento de crímenes utilizando las TIC.
• Robo de identidad digital: sustracción de información personal o de entidades, para realizar actividades no autorizadas.	• Deficientes controles para monitorear actividades sospechosas.

Fuente: Autoría propia

2.2 Determinación de los principales riesgos cibernéticos

Una vez identificadas las principales amenazas y vulnerabilidades se determinan los principales riesgos relacionados.

Base técnica

La ISO 31000: Gestión de riesgos, es una herramienta muy útil en este proceso y proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones.

Para el caso se considera convenientes los tipos de riesgos siguientes: a) riesgo legal, se asocia a la perdida en que incurre la empresa al ser multados u obligados a indemnizar por daños ocasionados a tercero por incumplimiento legales; b) reputacional el efecto de la perdida se ve reflejado en el desprestigio, mala imagen, de la compañía; c) económico que afecta básicamente los beneficios monetarios; y d) riesgo financiero relacionados con la gestión financiera de las empresas. Es decir, aquellos movimientos, transacciones y demás elementos que tienen influencia en las finanzas empresariales: inversión, diversificación, expansión, financiación, entre otros; como se presentan a continuación en la tabla 4. Principales riesgos cibernéticos.

Tabla 4.

Principales riesgos cibernéticos.

Codificación	Riesgo	Tipo de riesgo
R01	Extraer información confidencial de un cliente para fines fraudulentos o delincuenciales.	Riesgo legal
R02	Ciber espionaje de información para descubrir datos como contraseñas y cuentas bancarias.	Riesgo reputacional y riesgo legal

R03	Que el personal no esté capacitado para combatir técnicas de ingeniería social sofisticadas.	Riesgo reputacional Riesgo legal Riesgo económico
R04	Que la firma sea víctima de actividades de ciber extorción	Riesgo legal Riesgo reputacional
R05	Que la ocurrencia de DoS provoque una ralentización de los servicios inhabilitando su funcionalidad.	Riesgo económico Riesgo reputacional
R06	Mala configuración de los sistemas de información, lo que incluye a servidores, firewall y otros sistemas.	Riesgo financiero
R07	No ser capaces de restaurar la situación después de un incidente.	Riesgo legal Riesgo reputacional Riesgo económico
R08	Administración fraudulenta de la información por algún miembro de la alta dirección o áreas estratégicas de la firma.	Riesgo financiero Riesgo legal Riesgo reputacional
R09	Pérdida de información por robo de equipo, robo de contraseñas, fallos en el equipo (teletrabajo).	Riesgo financiero
R10	Pérdida o robo de información resguardada en la nube.	Riesgo financiero Riesgo reputacional

R11	Pérdida de información por robo de dispositivos móviles, accesos no permitidos, robos de contraseñas.	Riesgo financiero Riesgo reputacional
R12	Redes e infraestructura: Daños, accesos no permitidos, robos de información, fallos;	Riesgo financiero Riesgo reputacional
R13	Accesos no permitidos a archivos de forma directa: mediante acceso al disco duro donde se aloja la información.	Riesgo financiero Riesgo legal Riesgo económico Riesgo reputacional
R14	Falta de controles de Conexiones permitidas y no permitidas, desde y hacia el equipo (computadoras, dispositivos móviles).	Riesgo reputacional Riesgo financiero Riesgo económico
R15	Infección en computadoras y dispositivos móviles por software malicioso.	Riesgo financiero Riesgo económico Riesgo reputacional
R16	Accesos no permitidos al código y panel de administración de la página web de la firma.	Riesgo legal Riesgo reputacional Riesgo financiero Riesgo económico

R17	Acceso de dispositivos no autorizados a la red.	Riesgo financiero Riesgo económico
R18	Uso de la información pública en redes sociales utilizadas por la firma por piratas informáticos para conseguir datos que faciliten el acceso a dispositivos móviles, computadoras, nube, y otros equipos o programas.	Riesgo reputacional Riesgo económico Riesgo financiero Riesgo legal
R19	Propagación de virus en la red de la firma de auditoría	Riesgo económico Riesgo financiero Riesgo reputacional
R20	Alteración y destrucción de respaldos de información de la firma de auditoría.	Riesgo económico Riesgo financiero Riesgo legal
R21	Accesos a respaldos en la nube por usuarios nos autorizados.	Riesgo financiero Riesgo económico Riesgo legal
R22	Que el recurso humano divulgué información de la firma de auditoría al navegar en internet.	Riego legal Riesgo reputacional Riesgo económico Riesgo financiero

R23	Pérdida de información por error en hardware.	Riesgo económico Riesgo financiero
R24	Divulgación de información confidencial de la firma por parte de un ex empleado.	Riesgo legal Riesgo reputacional

Fuente: Autoría propia

2.1 Análisis de los riesgos

a) Escala de medición del riesgo

El riesgo será medido atendiendo a la probabilidad de ocurrencia de un evento no deseado, sin considerar el impacto de un evento, ni las acciones y controles mitigantes. A partir de ello se obtendrá el riesgo inherente; que es el riesgo existente ante la ausencia de alguna acción que la dirección pueda tomar para alterar tanto la probabilidad o el impacto del mismo.

A continuación, se presenta una propuesta de escala de valoración de la probabilidad de ocurrencia del riesgo.

Tabla 5.
Valoración de la probabilidad de ocurrencia del riesgo.

Probabilidad de ocurrencia	**Valor asignado**	**Valor cualitativo**
Una vez de forma anual	1	Excepcional (inusual)
Una vez de forma semestral	2	Bajo (raro que suceda)
Una vez de forma trimestral	3	Media (posible)
Una vez de forma mensual	4	Alta (es probable)
Más de una vez mensual	5	Muy alta (recurrente)

Fuente: Autoría propia, a partir de: ISO 31000.

La valoración del impacto del riesgo ser realiza tomando en cuenta una valoración cualitativa en áreas como la reputacional, legal, financiera y económica. En la tabla 4, se muestra la valoración del impacto del riesgo.

Tabla 6.

Escala de valoración del impacto del riesgo.

Grado de impacto	Valor asignado	Valor cualitativo
Puede tener un pequeño o nulo efecto en la institución, sin dañar la reputación o afectarle significativamente a nivel económico.	1	Muy bajo
Causa daño en el patrimonio o imagen que se puede corregir a corto plazo y no afecta el cumplimiento de los objetivos estratégicos.	2	Bajo
Causaría pérdidas patrimoniales importantes; incumplimientos normativos; se requeriría un tiempo significativo de la alta dirección para investigar y corregir daños; daño directo a la reputación de la firma.	3	Medio
Dañaría significativamente el cumplimiento de la misión, visión y objetivos; pérdidas patrimoniales; incumplimientos normativos; se requeriría un tiempo significativo de la alta dirección para investigar y corregir daños; daño directo a la reputación de la firma.	4	Alto
Influye directamente en el cumplimiento de la misión, visión y objetivos; pérdidas patrimoniales;	5	Muy alto

Grado de impacto	Valor asignado	Valor cualitativo
incumplimientos normativos; dejando sin funcionar por un tiempo importante los servicios que presta.		

Fuente: Autoría propia, a partir de: ISO 31000;

2.4 Valoración del nivel del riesgo

Se obtendrá a través de la multiplicación de la probabilidad de ocurrencia del riesgo y el impacto obtenida a partir de la escala de valoración del impacto del riesgo. Tal y como se muestra en la tabla 8. Escala de ponderación del nivel de riesgo. Además, en la tabla 7 se muestra la interpretación de los posibles resultados, que van desde 0 a 25.

Tabla 7.

Escala de valoración del nivel del riesgo.

Tipo de riesgo	Valor del nivel del riesgo	Tratamiento del riesgo
Riesgo grave	Nivel de riesgo menor o igual a 25 y mayor o igual a 15	Requiere la atención inmediata y máxima de la alta dirección y las partes involucradas, que permitan tomar las acciones convenientes contra el riesgo.
Riesgo alto	Nivel de riesgo menor a 15 y mayor o igual a 10	Se necesitan acciones urgentes de mitigación del riesgo.
Riesgo moderado	Nivel de riesgo menor a 10 y mayor o igual a 5	Será necesario medidas rápidas que permitan reducir el riesgo a bajo o mínimo

Riesgo bajo	Nivel de riesgo menor a 5 y mayor o igual a 2	El riesgo se mitiga con actividades preventivas
Riesgo mínimo	Nivel de riesgo menor a 2 y mayor o igual a 0	El riesgo es aceptable y fácil de eliminar

Fuente: Autoría propia, a partir de: (Guamán, 2015). Diseño de un sistema de gestión de seguridad de la información para instituciones militares (tesis previa a la obtención del título de magister en gestión de las comunicaciones y tecnologías de la información). Quito, Colombia.

Tabla 8.

Escala de ponderación del nivel del riesgo.

Código del riesgo	Probabilidad de ocurrencia	Impacto	Ponderación del riesgo	Nivel del riesgo
R01	1	5	5	Moderado
R02	2	5	10	Alto
R03	4	4	16	Grave
R04	1	5	5	Moderado
R05	2	3	6	Moderado
R06	2	3	6	Moderado
R07	2	5	10	Alto

Código del riesgo	Probabilidad de ocurrencia	Impacto	Ponderación del riesgo	Nivel del riesgo
R08	3	4	12	Alto
R09	2	2	4	Bajo
R10	1	4	4	Bajo
R11	3	3	9	Moderado
R12	2	5	10	Alto
R13	2	4	8	Moderado
R14	2	2	4	Bajo
R15	3	3	9	Moderado
R16	2	5	10	Alto
R17	2	2	4	Bajo
R18	2	2	4	Bajo
R19	2	2	4	Bajo
R20	3	3	9	Moderado
R21	2	3	6	Moderado
R22	2	4	8	Moderado

Código del riesgo	Probabilidad de ocurrencia	Impacto	Ponderación del riesgo	Nivel del riesgo
R23	2	2	4	Bajo
R24	2	4	8	Moderado

Fuente: Autoría propia

Como parte de la evaluación de riegos cibernéticos se establece el siguiente mapa de calor compuesto por 5 categorías de probabilidad y ocurrencia; se entenderá por probabilidad de ocurrencia a la posibilidad que un riesgo se materialice.

A continuación, se presenta la ubicación de los riesgos de la tabla 7:

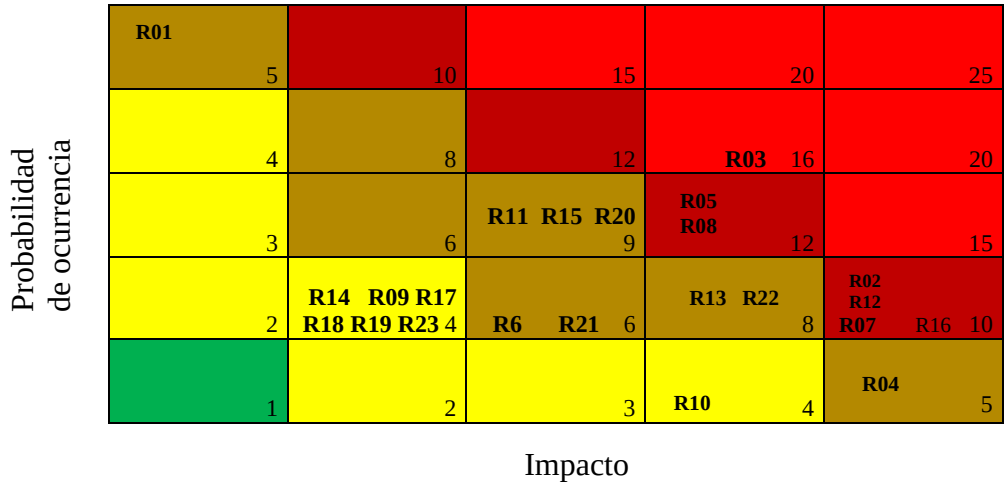


Tabla 9.

Mapa de calor del riesgo. Elaboración propia, a partir de: ISO 31000.

2.5 Plan de gestión de los riesgos

El plan de gestión de riesgos es una serie de actividades a seguir con la finalidad de reducir o mitigar el riesgo de ocurrencia de un evento. En la tabla 7 se muestra un detalle de actividades para cada uno de los principales riesgos identificados y el tipo de seguridad que se espera.

En donde “C” es confidencialidad, “D” disponibilidad e “I” es integridad.

Tabla 10.

Plan de gestión.

Código del riesgo	Nivel de riesgo	Opción de tratamiento	Actividad de mitigación	Tipo de seguridad		
				C	D	I
R01	Moderado	Reducir el riesgo	Establecer políticas de permisos, privilegios y/o control de acceso.	**X**		
R02	Alto	Reducir el riesgo	Cambios frecuentes de contraseñas, antivirus, utilización de programas anti rastreadores, y capacitación del personal contra estos ataques.	**X**		
R03	Grave	Reducir el Riesgo	Controles de acceso, cambios de contraseñas. Capacitaciones al personal.	**X**		
R04	Moderado	Reducir el riesgo	Realizar resguardos digitales de la información. (respaldos)	**X**		
R05	Moderado	Reducir el riesgo	Implementar métodos de defensa como: revisar configuración de firewall y routers para detener IP inválidas. Llevar control de logs para verificar conexiones en routers.			**X**

Código del riesgo	Nivel de riesgo	Opción de tratamiento	Actividad de mitigación	Tipo de seguridad		
				C	D	I
R06	Moderado	Reducir el riesgo	Invertir en software actualizados y con licencias originales	**X**	**X**	**X**
R07	Alto	Reducir el riesgo	Establecer medidas y normativa internas claras, que se den a conocer a todo el personal, proceso continuo de identificación y remediación de vulnerabilidades.	**X**	**X**	**X**
R08	Alto	Reducir el riesgo	Preguntar para que se necesita la información, comprobar las fuentes que solicitan la información, tener un grado de paranoia, control de privilegios administrativos.	**X**		**X**
R09	Bajo	Reducir el riesgo	Copias de respaldo de documentos, mantener servicios de sincronización en la nube, existencia de un protocolo que establezca cómo actuar al trabajar en remoto en lo que a seguridad se refiere, uso de	**X**		**X**

Código del riesgo	Nivel de riesgo	Opción de tratamiento	Actividad de mitigación	Tipo de seguridad		
				C	D	I
			escritorios remotos, cifrado de información.			
R10	Bajo	Reducir el riesgo	Crear contraseñas seguras (letras, números, mayúsculas, minúsculas), cifrar los archivos antes de subirlos, verificaciones de cuentas.	**X**		
R11	Moderado	Reducir el riesgo	Proteger los dispositivos con software de seguridad, autentificaciones del usuario con contraseñas, configuración de dispositivos para evitar redes inalámbricas que no sean seguras.	**X**	**X**	**X**
R12	Alto	Reducir el riesgo	Cifrado de datos confidenciales, incluyendo correos electrónicos; medidas de seguridad de la red (firewalls de nueva generación, *routers* y *switches* actualizados); aislamientos de redes (red para invitados); medidas de	**X**	**X**	**X**

Código del riesgo	Nivel de riesgo	Opción de tratamiento	Actividad de mitigación	Tipo de seguridad		
				C	D	I
			prevención de pérdidas de datos (DLP); copias de seguridad y pruebas de restauración periódicamente.			
R13	Moderado	Reducir el riesgo	Cifrado de archivos sensibles, cifrado de disco, de contenedor o de disco virtual	**X**	**X**	**X**
R14	Bajo	Reducir el riesgo	Cortafuego basado en host			**X**
R15	Moderado	Reducir el riesgo	Instalación de antivirus gratuitos o pagados, restricción de instalación de aaps no oficiales, contraseñas de inicio de sesión	**X**	**X**	**X**
R16	Alto	Reducir el riesgo	Actualización de CMS, plugin, plantillas, contraseñas seguras, auditoría de vulnerabilidades de la página web (en caso de desarrollo propio), copias de seguridad del sitio web.	**X**	**X**	**X**
R17	Bajo	Reducir el riesgo	Gestionar activamente todos los dispositivos hardware en la red,	**X**		**X**

Código del riesgo	Nivel de riesgo	Opción de tratamiento	Actividad de mitigación	Tipo de seguridad		
				C	D	I
			inventario de dispositivos autorizados y no autorizados.			
R18	Bajo	Reducir el riesgo	Manejo de redes sociales por personas formalmente autorizadas. La información a compartir debe ser estrictamente verificada antes de postearla, compartirla o subirla;	**X**		
R19	Bajo	Reducir el riesgo	Configuración de acceso limitado a redes y monitoreo de puertos y jerarquización de redes.			**X**
R20	Moderado	Reducir el riesgo	Actualización frecuente de respaldos, almacenamiento interno de respaldos con control de acceso, almacenamientos externos de respaldos en ubicaciones diferentes a la de la firma, capacitación a usuarios		**X**	**X**

Código del riesgo	Nivel de riesgo	Opción de tratamiento	Actividad de mitigación	Tipo de seguridad		
				C	D	I
			respectivos en el proceso de restauración de datos.			
R21	Moderado	Reducir el riesgo	Determinación de niveles de acceso, política de respaldo de la base de datos.	**X**		
R22	Moderado	Reducir el riesgo	Bloqueo de acceso a páginas de internet no seguras, firewall, chequeo del tráfico de red, políticas de acceso a internet.	**X**		
R23	Bajo	Reducir el riesgo	Adquirir equipos de cómputo de alta calidad con perfil empresarial, realizar pruebas de esfuerzo en los equipos de cómputo antes de renovarlos.		**X**	**X**
R24	Moderado	Reducir el riesgo	Firmas del personal de actas de confidencialidad, verificación que usuarios y contraseñas no se encuentren activas.	**X**		

Fuente: Autoría propia

FASE 3: PLAN DE ACCIÓN

Introducción

La información es el activo más valioso con el que cuentan las organizaciones, las firmas de auditoría no son la excepción a menudo disponen de ella para la realización de los encargos de auditoria, por lo que resulta importante adoptar lineamientos que permitan la protección de las misma; pues, con el uso de herramientas tecnológicas para la transmisión y resguardo de la información esta se vuelve vulnerable y susceptible de ser obtenida por terceros mal intencionados.

Por este motivo resulta importante para las firmas de auditoría preservar la seguridad cibernética de los datos que se comparten en el ciberespacio, y crear una infraestructura tecnológica que brinde un ambiente de control ante amenazas, riesgos y vulnerabilidades.

Objetivo

Las políticas de gestión de riesgos cibernéticos tienen como objetivo sugerir lineamientos para la protección de la información, de los riesgos cibernéticos a las que está expuesta la firma de auditoria debido al uso del ciberespacio, en consonancia con la gestión estratégica que poseen las firmas de auditoría y fundamentada en una serie de informes y marcos relacionados con la gestión del riesgo cibernético.

Como referencia se han tomado informes de firmas de auditoría con representación internacional y marco de infraestructuras críticas, rescatando de cada uno, aspectos relevantes que se adecuen a la realidad de las firmas de auditoría de El Salvador. Se debe agregar que la política de gestión de riesgo contiene: a) procedimientos de prevención, protección y detección; b) respuesta y comunicación y c) recuperación y aprendizaje.

Alcance

Las políticas de gestión de riesgos cibernéticos apoyan la gestión estratégica de la junta directiva, y es responsabilidad del comité de ciberseguridad. Debe ser aplicada por todo el personal de la firma de auditoría, desde la alta gerencia, administrativos, sénior de auditoria, asistentes de auditoria, y terceros que tengan acceso permanente o temporal a los sistemas de información y hardware.

3.1 Políticas y procedimientos para la gestión del riesgo cibernético

3.1.1 Lineamientos generales.

La ciberseguridad en las firmas de auditoría contribuye a aumentar la confianza de los clientes y obtener nuevos encargos de auditoria debido a la protección y seguridad de la información que se les brinda, todo ello implica un esfuerzo mutuo desde la alta gerencia hasta los colaboradores, ya no es un tema que corresponde exclusivamente al departamento o gerencia de TI, sino que debe ser parte de la gestión estratégica de la organización.

- **Creación de un comité de ciberseguridad.**

El comité de ciberseguridad será el responsable de la gestión de los riesgos cibernéticos de la firma de auditoría, materializando directamente el enfoque empleado por la junta directiva, quien dependerá orgánicamente de la misma.

Para la creación del comité de ciberseguridad se debe tomar en cuenta que los miembros sean profesionales responsables y comprometidos con el desarrollo de la firma.

Se sugiere que los miembros del comité sean profesionales que tengan conocimientos en tecnologías de la información, redes, telecomunicaciones, gestión de riesgos, manejo de recurso humano, auditoria, control interno y con conocimiento de leyes relacionadas a la seguridad de la información y el uso de tecnología; por lo que el comité puede ser conformado por ingenieros informáticos conformado por ingenieros informáticos , auditores, licenciados

en contaduría pública y administración de empresas. Se presenta la siguiente estructura orgánica para el comité:

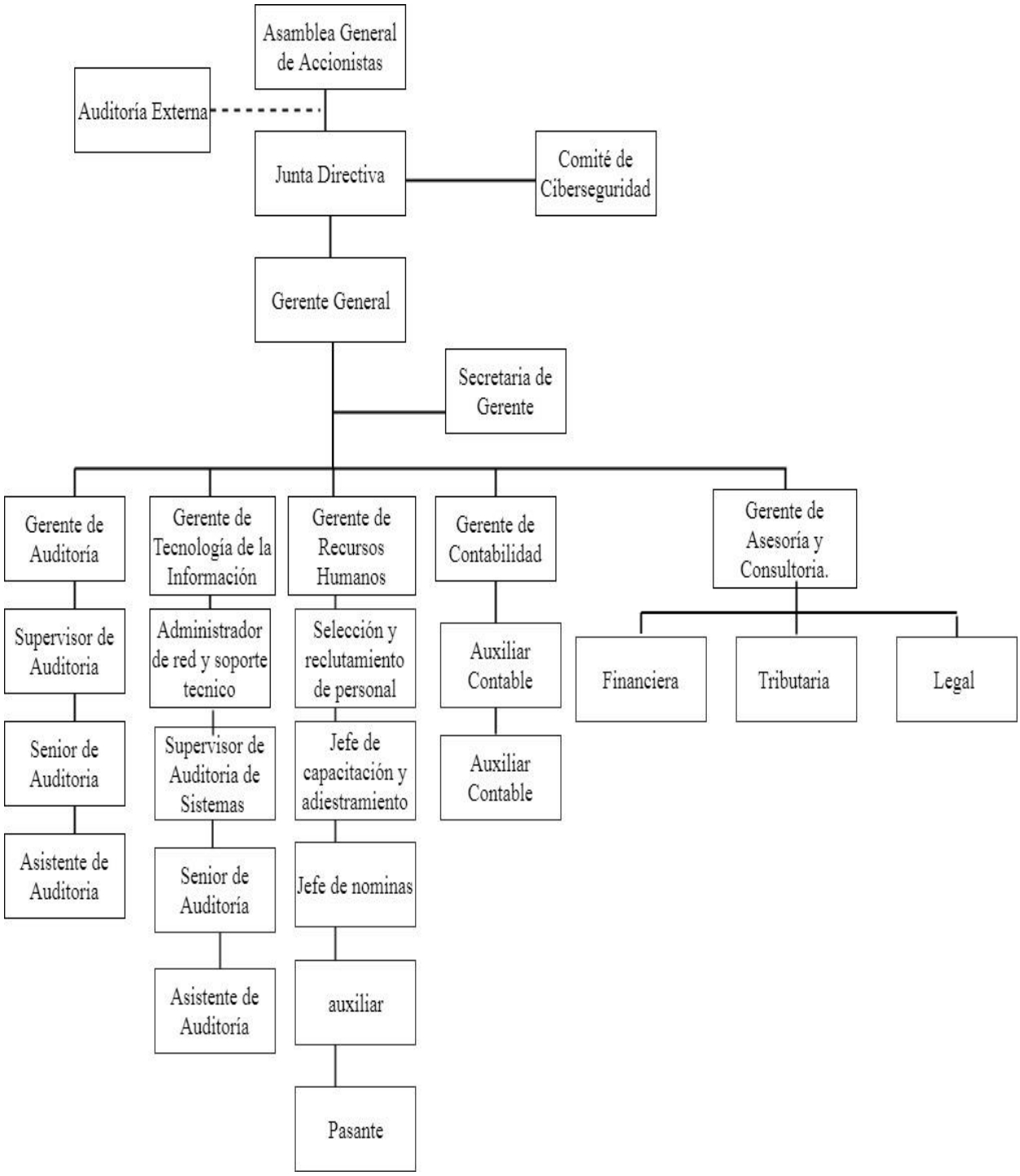


Figura 11. Estructura organizacional del comité de ciberseguridad.

- **Organización del comité.**

El comité de ciberseguridad dependerá orgánicamente de la junta directiva y se conformará de la siguiente manera:

Organización

Cargo	Profesión	Responsabilidad	Unidad Orgánica Dependiente
Gerente/técnico de TI	Ingeniero en sistemas o en informática	Presidente	Gerencia de TI
Socio o empleado	licenciatura en contaduría pública	Secretario	Gerencia de Auditoría.
Socio o empleado	licenciatura en contaduría pública	Vocal	Gerencia de Auditoría.
Socio o empleado	Licenciatura en administración de empresas.	Vocal	Gerencia de recursos humanos.

- **Responsabilidad del comité.**

Implementar la guía de gestión de riesgos cibernéticos, monitorear el cumplimiento, desarrollar el apetito del riesgo cibernético de la firma de auditoría, así como, identificar e informar a la unidad dependiente acerca de los riesgos y sugerirle propuesta de mejora. Además, se le asignan responsabilidades de:

- Es responsabilidad del coordinador del Comité verificar mediante la elaboración de un check list los incidentes de seguridad.

- Es responsabilidad de comité de ciberseguridad definir el protocolo de respuesta a incidentes. Realizando evaluaciones periódicas trimestrales, presentando el respectivo informe a junta directiva.
- Realizar el plan de capacitación para los empleados, y presupuestos para inversión en materia de ciberseguridad.
- Presentar a la junta directiva propuesta e iniciativas de mejora a la ciberseguridad.
- Realizar auditoría por lo menos una vez al año al área de tecnología de la información y comunicación con el propósito de verificar el cumplimiento de políticas y procedimientos.
- Investigar, diseñar y difundir boletines informativos acerca del uso de las tecnologías de la información a los empleados de la firma de auditoría.
- Verificar que los controles de accesos permitidos por el área de informática a los empleados sean adecuados al cargo que desempeña el empleado.
- Realizar inspecciones periódicas a las diferentes áreas de trabajo de la firma de auditoría para verificar el cumplimiento de políticas.
- Investigar, analizar y proponer mejoras en procesos deficientes aplicados por en departamento de informática.
- Investigar, estudiar y difundir al recurso humano aspectos legales relacionados con delitos cibernéticos en El Salvador.
- Comunicar a la junta directiva inmediatamente cualquier violación a los sistemas y equipos informáticos.

- **Junta directiva.**

Es la unidad encargada de la dirección de la gestión del riesgo cibernético e incluirlo en la planeación estratégica de la firma de auditoría.

  - **Responsabilidad.**

Autorizar la adopción de la guía de gestión de riesgos cibernéticos, la inversión en recursos humanos, herramientas y mejoras que permitan hacer una evaluación del riesgo de manera eficiente y eficaz, así como realizar actualizaciones de la guía y la evaluación del trabajo del comité de ciberseguridad.

Será responsabilidad directa de la junta directiva en adelante JD lo siguiente:

  - La aprobación e implementación de la guía de gestión de riesgos cibernéticos para la firma de auditoría.
  - Implementación y el cumplimiento de la presente política por parte del comité de ciberseguridad y los demás colaboradores.
  - Identificar, manejar y comprender los riesgos cibernéticos a los que está expuesta la firma de auditoría.
  - Seleccionar y designar a miembros que conformaran el comité de ciberseguridad.
  - Junta directiva es responsable de definir el equipo que integra el comité de ciberseguridad y designar las funciones de cada uno.
  - Incorporar en la gestión estratégica el riesgo cibernético al nivel del riesgo financiero y comercial.
  - El presupuesto asignado para gestionar el riesgo cibernético, será aprobado por Junta directiva y deberá incluir los programas de formación de los colaboradores.

- **Compromiso de la junta directiva.**

Comprensión clara del manejo de los riesgos cibernéticos de la firma por medio de la guía de gestión, consideraciones específicas del uso de la tecnología, debido a que los riesgos, las prioridades y los sistemas de cada negocio son únicos, las herramientas y métodos utilizados para el cometimiento del ciber delito, varía de acuerdo al tipo de atacante a que se enfrente por lo que la alta dirección debe estar alerta y actualizar procedimientos si es necesario y así mantener la información protegida de los nuevos ataques.

- **Principios.**

1. Flexibilidad: consiste en la capacidad de adaptar los procedimientos o políticas de gestión de riesgo a los avances tecnológicos recientes de la presente guía de gestión.

2. Trabajo en equipo: unión de esfuerzos de socios, junta directiva, comité de ciberseguridad y empleados para la alcanzar la protección de la información que interactúa en el ciberespacio.

3. Responsabilidad: la capacidad de cada parte interesada de cumplir con las funciones definidas en esta guía.

4. Competencia: mantener las capacidades, habilidades, conocimientos de leyes y marcos técnicos al nivel necesario para la aplicación de procedimientos de protección de la información, así como también las necesidades de formación.

- **Bases sobre las que se cimienta la ciberseguridad.**

Para la protección de la información de la firma de auditoría por medio de la gestión del riesgo cibernético, AGR Auditores tendrá presente que la ISO 27001 define 3 principios importantes que se describen a continuación:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Mentalidad en ciberseguridad.**

AGR Auditores, S.A. de C.V., integra en los valores, actitudes y prácticas de gobierno corporativo la mentalidad de ciberseguridad que incluye, priorizar en hábitos de los empleados como usuarios de la tecnología y de dispositivos interconectados (IOT), profesionales responsables de la gestión del riesgo y actores en el ecosistema en la seguridad de la información del ciberespacio. De manera que aumente la resiliencia de la entidad a las amenazas de la seguridad.

- Gobierno corporativo: examina que todas las áreas y niveles de gobierno han integrado una mentalidad de ciberseguridad.
- Comité de ciberseguridad: responsable de los procedimientos de ciberseguridad y comunicador de buenas prácticas de los empleados para el uso de los dispositivos tecnológicos en los que se almacena la información.

- **Aspectos legales.**

El comité de ciberseguridad de la firma de auditoría es el responsable del estudiar el contenido del marco normativo relacionado a la gestión del riesgo cibernético, así como la creación de políticas y procedimientos de cumplimiento de las mismas. A continuación, se describen cada una de las leyes relacionadas con delitos informáticos vigentes en El Salvador.

- **Ley Especial Contra los Delitos Informáticos y Conexos.**

Desarrolla los principales riesgos cibernéticos que enfrentan las empresas, entre los que se mencionan: robo de la información, manipulación de datos, fraudes y extorsión. La firma de auditoría por medio del comité de ciberseguridad estudia el contenido de la presente ley para luego difundir la información a los empleados de todos los niveles de la organización.

- **Ley de Firma Electrónica.**

Permite crear un clima de confianza entre los usuarios, debido a la protección de datos personales o propios de una entidad permitiendo garantizar la seguridad de la información por medio de los principios de autenticidad, integridad, confidencialidad, no repudiación y equivalencia funcional. La firma de auditoría gestionará los procedimientos necesarios para la obtención de la misma.

- **Ley de Propiedad Intelectual.**

Ley de propiedad intelectual de El Salvador tiene trascendencia en la ciberseguridad, debido al uso de software o código fuente proporcionados por terceros en los que se deben cumplir con los contratos celebrados y respetar los derechos de autor. La firma de auditoría debe de contar con una lista de elementos que están dentro del alcance de la presente ley y determinar procesos de protección a los mismos.

3.1.2 Procedimientos de prevención, protección y detección de riesgos

- **Actividades de apoyo y recursos.**

Las actividades de reducción del riesgo requieren la asignación de recursos dedicados y apropiados para su implementación, los recursos deben definirse en términos de dinero es decir un presupuesto dedicado, personas, materiales e infraestructura. La asignación de recursos consistentes y continuos proporciona las bases para una eficaz gestión de riesgo cibernético.

- **Recursos humanos.**

Para asegurar que la gestión del riesgo cibernético se lleve a cabo de manera eficiente y eficaz la firma de auditoría debe de contar con el personal idóneo y competente, necesario para la implementación de la guía de gestión. Para ello el comité de ciberseguridad debe estar conformado por profesionales expertos en informática, redes, telecomunicaciones y con conocimientos de planeación, evaluación, gestión de riesgos y talento humano capaces de dirigir y verificar el cumplimiento de las políticas de ciberseguridad.

a) Educación, capacitación y habilidades en ciberseguridad.

El comité de ciberseguridad en coordinación con la alta dirección debe de coordinar esfuerzos en cuanto a la educación de ciberseguridad en el entorno laboral, para ello se tomará en cuenta aspectos importantes que menciona el modelo de madurez de capacidades de ciberseguridad para las naciones (CMM). Las cuales se adaptan a las necesidades de la firma y que se detallan a continuación:

- Actividades de sensibilización: se centran en la permanencia y diseños de programas para mejorar la sensibilización de los empleados acerca de los riesgos y amenazas del ciberespacio y como abordarlos. La difusión de los correos electrónicos informativos que permitan al empleado estar al tanto de las implicaciones que tiene el uso de las redes y dispositivos interconectados es una opción.
- Difusión de prácticas de ingeniería social: aspecto al que se debe prestar atención pues los atacantes preparan técnicas que parecen inofensivas para extraer información, la firma de auditoría creara políticas para este tipo de prácticas.
- Capacitación profesional: implica el desarrollo de programas de capacitación que desarrolla el equipo profesional del comité de ciberseguridad liderado por la persona experta en talento humano y representante del departamento de recursos humanos.

- Provisión: este aspecto explora si existen ofertas educacionales en ciberseguridad fuera de la firma tales como capacitaciones, seminarios, material de estudio, cursos en línea entre otros, que satisfagan las necesidades actuales.
- Administración: este aspecto explora la coordinación de recursos para desarrollar los programas de educación al personal dentro y fuera de la firma, así como mejorar la guía de gestión de riesgos cibernéticos.

b) Plan de capacitaciones.

El comité de ciberseguridad es responsable de realizar un plan anual de capacitación para ser presentado a la junta directiva para su aprobación, este plan formara parte de la guía de gestión de riesgos cibernéticos.

- El plan de capacitación en ciberseguridad debe incluir a todos los empleados de la firma desde los altos directivos hasta los colaboradores.
- Cuando se contrate personal nuevo al recibir la capacitación de inducción debe incluir el tema de ciberseguridad y dar a conocer las políticas de la presente guía de gestión.
- Comunicar al personal el día, fecha, lugar y hora de la capacitación para que asista con puntualidad. Proporcionar, además, el material didáctico necesario para el desarrollo de actividades.
- Los empleados nuevos deben de leer, comprometerse, leer y firmar un acta de confidencialidad.

c) controles de acceso.

- Los privilegios para modificar la funcionalidad, conectividad y dispositivos de seguridad tales como firewalls, acceso a internet y routers deberán ser restringidos a un grupo mínimo de empleados permanentes, de confianza y con amplios conocimientos en el tema. Los privilegios los concederá el gerente de TI quien será

el custodio máximo de los accesos otorgados; quien estará bajo supervisión del comité de ciberseguridad.

- Cada miembro de la firma de auditoría que tenga asignado equipo informático se le proporcionará un nombre de usuario y deberá crear una contraseña tomando en cuenta lo establecido en la presente guía.
- Los accesos al sistema de proporcionaran de acuerdo al cargo que se desempeña en la firma, no se permitirán accesos que sean incompatibles.
- Por los menos una vez al año se debe de evaluar los accesos que tienen los usuarios para determinar si son los idóneos para el cargo desempeñado.
- Los empleados que dejen de trabajar para la firma de auditoria se le deberán restringir todo tipo de acceso que se le haya proporcionado.
- Gestión de privilegios de usuarios: definir privilegios para cada tipo de usuarios, restringir tareas y configuraciones del equipo con permiso y contraseña del administrador.
- En casos de ceder privilegios a los usuarios estos se debe de comunicar por escrito definiendo claramente las responsabilidades y el tiempo que se concederá.
- Verificar que las cuentas de usuario tienen acceso autorizado y no cuenten con privilegios de aplicaciones.

- **Logs.**

Todo cambio que se realice a los parámetros de configuración de reglas, rutas de acceso, actividad sospechosa que, de indicios de accesos no autorizados, deberán ser registradas en un log.

- Los logs deberán ser revisados periódicamente por el jefe del departamento de TI, así mismo el comité de ciberseguridad tendrá la facultad para hacer las revisiones respectivas.
- Se debe de proteger la integridad de los logs mediante la encriptación y deben ser respaldados de forma segura.

c) Contraseñas

En las firmas de auditoría se hace uso de una serie de accesos a cuentas y/o equipos, para ello se debe hacer uso de contraseñas, para lo cual deben tomar en consideración los siguientes aspectos:

- La contraseña para el acceso a cuentas de sistemas o programas de auditoría, contables o equipos proporcionados por la firma tales como computadoras, tabletas o teléfono celular deben ser diferente debido a que, si un atacante tiene acceso a ella, tendría la llave para toda la información.
- Utilizar un administrador de contraseñas para que almacene y encripte todas las contraseñas complejas y diferentes que son difíciles de recordar por los usuarios.
- Para acceder al administrador de contraseñas de debe crear una contraseña maestra para cada una de las cuentas de usuario y las contraseñas utilizadas por los empleados.
- La contraseña debe tener una longitud mínima de 8 caracteres, pero no más de 64 evitando utilizar contraseñas comunes que se pueden adivinar con facilidad; por ejemplo, contraseña o abc123.
- Para crear una buena contraseña se debe evitar utilizar oraciones comunes y famosas, palabras del diccionario, nombres o errores ortográficos comunes.
- Al crear una contraseña, para que sea robusta se debe de utilizar una frase en lugar de una palabra, eligiendo una oración que signifique algo para sí.

- Las contraseñas asignadas a los equipos proporcionados por la firma de auditoria se deberán cambiar por lo menos cada tres meses.
- Realizar el cambio de contraseñas en caso de robo de los dispositivos asignados.

d) Funciones básicas de los empleados.

- Los dispositivos que el personal utilice para el acceso a la cuenta de correo electrónica corporativa deberá tener contraseña, actualización de antivirus, así como se deberá acceder desde redes seguras y siempre deberán estar bajo el cuidado del Técnico de TI.
- Los colaboradores nuevos en la organización deben recibir instrucciones sobre la configuración cifrada, las contraseñas, la instalación y actualización del antivirus.
- Cuando se brinde conexión y acceso a internet en oficinas del cliente, se deben asegurar que la red sea segura para iniciar sesiones en la cuenta.
- El área de informática es responsable de atender todas las inquietudes del equipo de auditoria frente a correos o y/o procesos que deban surtir en sus equipos, con el fin de prevenir procesos que representen un riesgo para la organización y comunicar al comité.
- Los colaboradores deberán cumplir con las siguientes acciones para mitigar las violaciones de seguridad:
    a. Apagar sus equipos y/o bloquearlos cuando se retiren de sus escritorios o finalice su jornada de trabajo.
    b. Reportar la pérdida o daño de los dispositivos asignados en el menor tiempo posible al área de informática, de manera escrita por medio de un correo electrónico.

c. Identificar amenazas a la información y notificarlas al comité de ciberseguridad.

d. Para evitar contaminar el equipo de virus o algún tipo de malware se restringirá el acceso a páginas web que no sean necesarias para la realización de los encargos de auditoria.

e. Los usuarios no deberán abrir adjuntos de correos electrónicos, a menos que sean enviados por una fuente confiable y se implementarán medidas para bloquear archivos adjuntos de correo electrónico con comportamiento sospechoso.

f. Las violaciones intencionales, recurrentes o de gran escala, llevarán a tomar acciones disciplinarias que inclusive pueden ser justa causa para la terminación del contrato.

e) Tratamiento de la información que dispone la firma.

- La información proporcionada por los clientes del encargo de auditoria, deberá ser utilizada únicamente por el equipo responsable y queda terminantemente prohibido que dicha información sea utilizada con fines personales o educativos por el personal de la firma.
- Las computadoras que tienen asignados los miembros de la firma de auditoria no permitirán conectar dispositivos portátiles tales como USB y CD en los que pueden sustraer información y ser compartida con terceros.
- La elaboración de papeles de trabajo y archivos debe ser en las instalaciones de la firma de auditoria o durante las visitas programadas al cliente del encargo, por ningún motivo un empleado debe llevarse archivos para el hogar y fuera del horario laboral.

- Los papeles de trabajo por algún motivo se sustituyan a causa de errores debe ser triturara o destruida de forma segura para evitar que por descuido se revele información de los clientes o de la firma.
- La información que se transmite por páginas web o redes sociales primero debe ser revisada por el comité de ciberseguridad, para luego proceder a publicarla.
- Las políticas y procedimientos deben de ser comunicados al personal de la firma ya sea de forma escrita o mediante correo electrónico.
- Cifrado de archivos sensibles, cifrado de disco, de contenedor o de disco virtual**.**
- Los soportes físicos que almacenan información por ningún motivo se deben de reutilizar, vender, regalarlo o simplemente desecharlo sin realizar el borrado seguro.
- Para desechar soportes físicos de información se debe realizar por medio de la destrucción física por medio de una destructora de papel o de medios magnéticos.

- **Recursos Financieros.**

Para el buen funcionamiento de la gestión de riesgos es importante contar con recurso humano competente en la materia, sin embargo, la asignación de recursos financieros para tal fin es necesaria por lo que la firma de auditoría proporcionará los recursos. Algunos desembolsos en los que se pueden incurrir son los siguientes:

- Actividades de capacitación en lugares ajenos a la firma de auditoría.
- Licencias de software y antivirus.
- Inversión en *routers* de servicios integrados (ISR) o dispositivos IPS de nueva generación que permitan el filtrado de tráfico, la capacidad de ejecutar un sistema de prevención de intrusiones, cifrado y las capacidades de VPN para las conexiones de cifrado seguro.

- **Conexión de dispositivos redes e internet.**

a) **Internet y redes.**

- En la firma de auditoría se debe evaluar mediante la elaboración de check list el nivel de confianza y seguridad en el proveedor de los servicios de internet.
- Todo empleado que se le brinde acceso a internet deberá cumplir y respetar con las Políticas y procedimientos establecidos en la presente guía.
- Tendrán acceso a internet solo aquellos empleados autorizados por la firma de auditoria por medio la junta directiva en coordinación con el departamento de TI.
- Se debe evitar el uso personal de servicios de internet, servicios de mensajería, descargas que no estén autorizadas por el departamento de TI.
- Todas aquellas redes no controladas por el departamento de TI de la firma serán consideradas inseguras (redes públicas o extranet).
- La única forma de acceso a internet es la proporcionada por la firma, la red privada quedando prohibido la utilización de módems.
- Los empleados que se conecten a internet deben utilizar mecanismos seguros y encriptados de acceso y autenticación.
- Bloqueo de sitios: se bloquearán y restringirán sitios de internet ofensivos, de distracción y potencialmente dañino para el funcionamiento del equipo. Tales como: Facebook, WhatsApp, YouTube y páginas pornográficas.
- La firma de auditoria debe de contar con una lista documentada de accesos y equipos permitidos para la conexión a la red, esta debe ser elaborada por el departamento de TI, y distribuida a los administradores de redes.

- Toda ruta de conexión que no esté permitido en la lista documentada deberá ser bloqueado por el administrador de redes, en este caso el comité de ciberseguridad verificara el cumplimiento de dichos procedimientos.
- Las redes inalámbricas permiten que los dispositivos habilitados con Wi-Fi, como computadoras portátiles y tablets, se conecten a la red por medio de un identificador de red conocido como Identificador de Conjunto de Servicios (SSID).
- Para evitar que los intrusos ingresen a las redes inalámbricas, el SSID predeterminado y la contraseña predeterminada para la interfaz de administración en el navegador web deben cambiarse.
- Encriptar la comunicación inalámbrica habilitando la seguridad inalámbrica y la función de encriptado WPA2 en el *router* inalámbrico.
- Los dispositivos portátiles proporcionados por la firma de auditoría, solo deben conectarse a la red privada de la misma. En caso de visitas de auditoria en las oficinas del cliente, a la red privada del cliente si fuere necesario.
- En caso se haga uso de una red pública, para evitar que una persona intercepte la información se debe de utilizar túneles VPN y servicios encriptados, este proporcionara acceso seguro a Internet con una conexión cifrada entre la computadora y el servidor VPN del proveedor de servicios. sí en caso se intercepte la información, no podrá descifrarse.
- Mantener el Bluetooth apagado cuando no se utiliza.

b) **Escaneo de puertos.**

Consiste en un proceso de comprobación de una computadora para conocer los puertos abiertos. Para la firma de auditoría es importante conocer las mayores posibilidades de un robo de información por lo que se debe de evaluar el firewall de la red de las computadoras

y la seguridad de los puertos, para ello se puede hacer uso de una herramienta de escaneo de puertos, llamada Nmap, no debe realizarse en servidores públicos en Internet o en la red de una empresa sin permiso.

El escaneo de puertos generalmente provoca alguna de estas tres respuestas:

- Abierto o aceptado: el host respondió e indicó que hay un servicio activo en el puerto.
- Cerrado, denegado o no escucha: el host respondió e indicó que se denegarán las conexiones en el puerto.
- Filtrado, caído o bloqueado: no hubo respuesta del host.

c) **Jerarquización de redes.**

- Dividir la red en capas independientes tales como capa de acceso, de distribución y central de manera que permitan administrar el trafico local.
- El departamento de TI de la firma de auditoría es el encargado del diseño jerárquico de las redes.

d) **Dispositivos interconectados.**

- Los dispositivos deberán correr versiones actualizadas de sistema operativo y de software; suscritos a mantenimiento y servicios de actualización que brinde el proveedor.
- La firma de auditoría deberá proteger la información que se transmite por medio de diferentes dispositivos interconectados, contra intrusiones. Para ello debe seguir los siguientes pasos:

a) M**antener el *firewall* encendido:** ya sea un firewall de *software* o un *firewall* de *hardware* en un *router*, debe estar activado y actualizado para evitar que los *hackers* accedan a datos de la firma, empleados y clientes.

b) **Utilizar un antivirus y *antispyware:*** el software malicioso, como virus, troyanos, gusanos, *ransomware, malware, phishing* y *spyware,* se instala en los dispositivos informáticos sin permiso para obtener acceso a computadoras.

c) **Administración del sistema operativo y navegador**: mantener actualizado el sistema operativo de las computadoras, incluidos los navegadores web, descargar e instalar periódicamente parches y actualizaciones de seguridad del software de los proveedores.

d) **Proteger todos los dispositivos:** dispositivos informáticos, ya sean PC, PC portátiles, *tablets* o *smartphones,* deben estar protegidos con contraseña para evitar el acceso no autorizado de la siguiente manera:

   - La información almacenada debe estar cifrada, especialmente en el caso de datos sensibles o confidenciales.
   - En los casos que la firma proporcione a los empleados dispositivos móviles, solo deben almacenar la información necesaria para no comprometer la seguridad de la información en caso de robo o extravío.
   - Si se planea adquirir dispositivos del IoT (Internet de las cosas), se debe considerar que representan un riesgo incluso mayor que los otros dispositivos electrónicos. Mientras que las computadoras de escritorio, sportátiles y los dispositivos móviles reciben actualizaciones de software frecuentes, la mayoría de los dispositivos de IoT aún tiene su firmware original. La mejor manera de protegerse de esta situación es contar con dispositivos de IoT con una red aislada compartida únicamente con otros dispositivos de IoT.

e) **Antivirus.**

- Mantener en cada equipo antivirus instalado y actualizado con licencia del proveedor.
- Ejecutar cada cierto tiempo análisis completo a los equipos para determinar irregularidades y limpiar el equipo de archivos basura o que ralentizan los dispositivos.
- El antivirus debe de incluir programas anti rastreadores que permitan la protección del tráfico que entra y sale de los dispositivos.
- Seleccionar un antivirus que permita navegar de forma privada en la red, por medio del cifrado de la información que entra y sale.
- La entidad proveedora de la licencia de antivirus deberá contar con equipo de soporte técnico.

f) **Descargas.**

- Descargar software solamente de sitios web confiables para evitar obtener spyware, virus, gusanos y cualquier tipo de malware.

- **Realizar respaldo de datos**
  - La firma de auditoría debe de contar con respaldos de información para evitar la pérdida de datos irremplazables y garantizar la seguridad en caso de robo, incendio o cualquier otro acontecimiento.
  - Para utilizar los servicios de la nube es necesario leer las condiciones de uso en lo referentes a garantías de disponibilidad y confidencialidad de la información.
  - No se permite a todos los empleados de la firma subir y descargar información de la nube, a excepción de la o las personas que la alta dirección designe.

- Los datos que se van a subir a la nube primero deben ser cifrados, para ellos se puede contratar servicios que permitan cifrar la información antes de subirla.
- La frecuencia de los respaldos se debe de realizar de forma diaria para la base de datos de los sistemas, quincenal para las bases de datos de correo electrónico.
- la periodicidad de los respaldos de la información de los usuarios será de forma completa una vez al año de preferencia el último mes del año en curso.
- Los usuarios deben de mantener ordenada la información por carpetas con nombres cortos para facilitar el respaldo.
- Las carpetas históricas de exempleados no se respaldan.
- Disponer de copia de seguridad fuera de la firma de auditoría para evitar perdida de información en caso de incendio, inundación y robo.

- **Hardware.**
  - El departamento de informática tiene la responsabilidad de controlar y llevar un inventario detallado de la infraestructura de hardware de la firma.
  - El comité de ciberseguridad debe garantizar que el departamento de TI lleve un inventario actualizado del hardware.
  - El área de informática es el ente autorizado para definir los estándares a considerar en la adquisición de activos informáticos.
  - Solo podrán adquirirse los activos informáticos de alta calidad y que hayan sido autorizados en el plan de adquisiciones que debe llevar el departamento de informática, bajo la normativa y estándares aprobados y emitidos por el área de Informática.

- El mantenimiento técnico preventivo de todos los activos de infraestructura de tecnología de información de la Compañía, deberá ser realizado por el área de informática.
- El comité de ciberseguridad tendrá la facultad de revisar o estudiar la labor realizada por el departamento de informático y sugerir aspectos de mejora.

- **Software.**
  - El Software que se utilice en la firma de auditoria debe ser adquirido con licencias originales que cuenten actualización y soporte técnico.
  - Eliminación de software no autorizado: no descargar aplicaciones o programas de internet de dudosa procedencia, no confiable o no autorizado que puedan causar la degradación del equipo informático.
  - Todos los archivos descargados de internet deben ser analizados, antes de su uso mediante el uso del antivirus instalado por el departamento de informática.
  - Para las actualizaciones automáticas, los usuarios no deben de realizarlas incluso aquellas aplicaciones o sistemas que cuenten con licencia.
  - La firma de auditoría debe de adquirir un software que le permita controlar al acceso no autorizado al software mediante un gestor de alertas y el seguimiento por medio de una bitácora de las acciones realizadas.

- **Seguridad física.**

Para proteger el sistema de información de las amenazas del entorno de carácter físico la firma de auditoria implementara procedimientos que permitan la protección, resguardo y buen funcionamiento de los equipos y sistemas.

Para la seguridad física la ISO 27002:22005 proporciona una guía de procedimientos a seguir, para la firma de auditoria se definen y adaptan a la necesidad de la firma los siguientes:

- La firma de auditoria debe de identificar todos sus activos incluyendo los digitales, asignarles un propietario quien seguirá las reglas de uso.
- Realizar una clasificación de la información como negociable, sensitiva y crítica.
- El perímetro de seguridad debe evaluarse para proteger las áreas donde se almacenas los soportes de información.
- Se deben establecer controles físicos de entrada tales como el uso de carnet de visitantes, autorización para el acceso, comprobación de identidad, revisión del registro de visitas y registros de entrada y salida.
- Es obligación el uso de identificadores en el interior de la firma, además se debe llevar procedimientos adecuados para la emisión control, registro, baja y cancelación de identificadores.
- Los identificadores deben ser con diseños difícil de falsificar, con fotografías y accesos cerrados en horas no laborales.
- Verificación del control de llaves.
- Establecer procedimientos de amonestación por el uso de dispositivos en el sitio de trabajo e inhabilitar puertos USB.

- **Infraestructura.**

La entidad debe contar con software y hardware en buen estado y adecuado para la realización de encargos de auditoria y que cuenten con las medidas básicas de la seguridad de la información. Además de proporcionar a los empleados instalaciones cómodas, seguras y que les permitan la realización de las funciones de manera óptima.

- **Control de los documentos.**

Para controlar los documentos que resultan de la gestión de riesgos cibernéticos es importante que la firma de auditoría cuente con procedimientos, que le permitan definir las

acciones necesarias para el buen uso de la información, tomando en cuenta la ISO 27000 se detallan los siguientes:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están Identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

3.1.3 Procedimientos de respuesta y comunicación.

La firma de auditoría debe estar preparada para que en caso se desarrolle un incidente, el daño pueda ser lo menor posible.

El departamento de TI debe de comprender que un impacto de la violación de seguridad no solo está relacionado con el aspecto técnico, los datos robados, bases de datos dañadas, daños a la propiedad intelectual; los daños también se extienden a la reputación de la empresa, problemas jurídicos o comerciales, por lo que deben de dar cumplimiento a lo siguiente:

a) Cultura de ciberseguridad en la firma.

El elemento tecnológico requiere de una cultura de seguridad responsable por parte de toda la firma de auditoría, entendimiento de niveles de riesgos cibernéticos, confianza en los servicios de internet, uso de correo electrónico, transmisión de la información por parte de los clientes, almacenamiento en la nube y el conocimiento de los empleados de medidas de protección de datos personales y de información empresarial que se transmite por medio del uso del ciberespacio.

En este factor incluye la existencia de mecanismos comunicación de incidentes que operan como canales entre los empleados y el comité de ciberseguridad.

b) Comunicación en caso de una violación a la seguridad.

A continuación, se presentan algunas medidas importantes que la firma de auditoría debe adoptar cuando identifica una violación de seguridad, según muchos expertos en seguridad:

- Comunicar el problema: Informar internamente a los empleados del problema y llamarlos a la acción, el comité de ciberseguridad es el responsable de esta acción.
- Cuando los dispositivos de seguridad generen alertas de intrusiones, intentos de ataques o ataques materializados, los técnicos deben alertarse e informar por medio de correo electrónico, personalmente o cualquier otra forma de comunicación que garantice que el mensaje llegue al receptor quien será su jefe inmediato superior quien decidirá las medidas o tomar.
- Informar externamente a los clientes a través de comunicación directa y anuncios oficiales, la comunicación genera transparencia, que es crucial para este tipo de situación.
- Ser sincero y responsable en caso de que la firma tenga la culpa.

- Proporcionar detalles: explicar por qué ocurrió la situación y qué se vio afectado, si es necesario se debe hacer cargo de los costos de los servicios de protección contra el robo de identidad para los clientes afectados.
- Comprender qué causó y facilitó la violación de seguridad, si el comité se le hace imposible identificarlo se debe de contratar un experto para que investigue y conozco los detalles del incidente.
- Modificar, eliminar o incorporar procedimientos con base en la experiencia.
- Asegurarse de que todos los sistemas estén limpios, que no se hayan instalado puertas traseras y que no haya nada más comprometido.

c) Cuestiones éticas.

Los empleados de la firma de auditoría deben de actuar con un código de comportamiento ético, apegado a los lineamientos internos de la misma y externo, como la regulación vigente.

En materia de ciberseguridad no existen leyes específicas que regulen, existen áreas que no están cubiertas por lo que se llegaría a pensar que se puede llegar hacer algo legal, pero, que no es ético. Las firmas de auditoría requieren de ética en la realización de encargos de auditoria para ello se cuenta con el código de ética de IFAC y con normas internacionales de auditoría que puntualizan en este aspecto.

d) Inversión en equipo para reforzar la seguridad.

- Routers: los routers de servicios integrados (ISR) tienen muchas capacidades similares a las de un firewall además de las funciones de ruteo, entre ellas, el filtrado de tráfico, la capacidad de ejecutar un sistema de prevención de intrusiones (IPS), el cifrado y las capacidades de VPN para las conexiones de cifrado seguro.
- Firewalls: dispositivos que permitan el análisis y administración de redes avanzadas.

- IPS: los dispositivos IPS de nueva generación, están dedicados a la prevención de intrusiones.
- VPN: dispositivos de seguridad que cuenten con tecnologías de redes virtuales privadas (VPN) tanto de cliente como servidor para establecer conexiones de cifrado seguro.

3.1.4 Recuperación y aprendizaje

Cuando en la firma de auditoría se detecte una violación a la seguridad, deben adoptarse las acciones adecuadas para minimizar el impacto y los daños.

Se debe contar con un plan de respuesta este debe ser flexible con múltiples opciones de acción durante la violación. Una vez contenida la violación y restaurados los sistemas y servicios comprometidos, las medidas de seguridad y los procesos de la guía de gestión de riesgos cibernéticos deben actualizarse para incluir las lecciones aprendidas durante la violación.

Toda esta información se debe recopilar en un libro de estrategias de seguridad. Un libro de estrategias de seguridad es un conjunto de consultas repetidas (informes) de fuentes de datos de eventos de seguridad que conducen a la detección y la respuesta ante los incidentes. El comité de ciberseguridad es el responsable de realizar el libro de estrategias para luego determinar las actualizaciones o modificaciones de procedimientos de la guía, luego presentarlas a la junta directiva para su aprobación. El libro de estrategias de seguridad debe cumplir las siguientes acciones: a) detectar equipos infectados con malware, actividad de red sospechosa e intentos de autenticación irregulares; b) describir y entender el tráfico entrante y saliente; c) proporcionar información de resumen que incluya tendencias, estadísticas y recuentos; d) proporcionar acceso rápido y utilizable a estadísticas y métricas; y e) establecer una correspondencia de eventos en todas las fuentes de datos relevantes.

FASE 4. IMPLEMENTACIÓN

4.1 Introducción

En esta fase se establecen un conjunto los procedimientos claves recomendados, orientados a reducir, mitigar, o eliminar los ataques comunes y dañinos por amenazas, vulnerabilidades o riesgos que afecte la confidencialidad e integridad de la información, en las diferentes áreas de la organización.

Se debe considerar a los procesos de gestión de ciberseguridad, como el centro de estrategia en la organización, ya que permite aumentar la confianza en la detección de un evento de ciberataque. Debe incluir las características siguientes: innovador, alineadas con la normativa legal aplicable, enfocada al recurso humano y riesgo.

A continuación, se detalla las principales áreas que brindaran un ambiente de seguridad a la organización:

Tabla 11.

Áreas que brindaran un ambiente de seguridad a la organización.

No.	ÁREA	PROCEDIMIENTO
1	Recursos Humanos	Realizar capacitaciones trimestrales sobre temas de interés como ciberseguridad o afines, con el propósito de concientizar y evitar que el personal sea víctima de sustracción de información clave de la entidad por terceros mal intencionado.
3	Internet, Conexión de dispositivos	Realizar periódicamente inspecciones físicas al equipo asignado al equipo de auditoria, para verificar su adecuado funcionamiento.
4	Software	Verificar que los software se mantengan actualizados, así mismo velar por el cumplimiento por las medidas de control ante amenazas cibernéticas detallas en la política de ciberseguridad.
5	Redes	Preservar la integridad y confidencialidad de la información compartida por medios conectados entre sí; que permiten continuar con las operaciones del negocio.

6	Hardware	Verificar periódicamente el buen funcionamiento del equipo proporcionado al personal, para la realización de sus actividades diarias.

4.2 Procesos de gestión de ciberseguridad

A continuación, se desarrolla los procesos para la gestión de ciberseguridad para la organización, en concordancia con el análisis de riesgos identificados en la fase 2; donde se debe referenciar los papeles de trabajo y la persona asignada para realizar dicho proceso.

Cabe señalar que los ejemplos citados a continuación su propósito es ilustrativo, ya que no pretenden abarcar todos los controles posibles que una organización puede implementar frente a los riegos en ciberseguridad, debe ser necesario que se determine la mejor práctica y control.

AGR, S.A. DE C.V.

PROCESOS PARA LA GESTIÓN DE CIBERSEGURIDAD

ÁREA: RECURSOS HUMANOS

OBJETIVO GENERAL:

Formar a los integrantes del encargo de auditoria y colaboradores de la organización en la identificación de posibles ataques cibernéticos a través de la utilización de las tecnologías de la información.

Evaluando trimestralmente a través de técnicas documentadas, entrevistas o cuestionarios que le permitan a la administración comprobar su desempeño ante posibles incidentes (tomando en cuenta los resultados anteriores para ser comparados).

No.	PROCEDIMIENTO	REF.	HECHO POR
1	Identificar la formación y conocimiento que requiere la organización de los colaboradores, para la implementación de acciones de seguridad.	**A1**	**YPR**
2	Formar a los colaboradores en la identificación de posibles ataques por medio de correo electrónico y acceso a internet.	**A1**	**YPR**

3	Asignar los talleres de formación de acuerdo al acceso que tenga a la información confidencial de los clientes, además del rol desempeñado dentro de la organización.	**A2**	**YPR**
4	Firmar Declaración de confidencialidad por parte del personal de la empresa, por lo menos una vez al año.	**A3**	**YPR**
5	Enviar periódicamente boletines informativos, correos de advertencia ante posibles casos de *phising.*	**A4**	**YPR**
6	Filtrar los correos electrónicos de usuarios ajenos al correo institucional de AGR, a través de mensajes de advertencia; permitiendo eliminar aquellos de procedencias sospechosas.	**A5**	**YPR**
7	Entregar un formulario que comprueba haber leído políticas y procedimientos de TI, a través de firma por parte de todos los empleados.	**A6**	**YPR**

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

A1

AGR, S.A. DE C.V.
MEMORÁNDUM GG-2019

De: Comité de ciberseguridad
Para: Jefe departamento Administrativo, Auditoria y TI.
Cc: Gerencia General; Gerencia de Recursos Humanos
Asunto: Cronograma de capacitaciones al personal 2019

Por este medio se les informa al personal de la empresa, que como medidas de prevención ante posibles incidentes de seguridad cibernética, se han asignado de acuerdo al cargo que desempeñan, la información confidencial que manejan, los diferentes cursos detallados a continuación:

No.	Nombre del curso	Fecha	Personal que asistirá
1	Introducción y visión general de la ciberseguridad	15/07/2019	Departamento Administrativo, Auditoria y TI.
2	Seguridad de redes, sistemas, aplicaciones y datos. Respuesta a incidentes de ciberseguridad.	20/08/2019	Departamento de TI
3	Principios de seguridad, Gestión de riesgos, Amenazas/ataques, Malware, Virus, Control de acceso, Seguridad de red y perimetral, Seguridad en internet.	01/09/2019	Senior de Auditoria y Departamento de TI.
4	Identificación de posibles ataques por medio de correo electrónico y acceso a internet.	25/11/2019	Departamento Administrativo, Auditoria y TI.

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

A2

AGR, S.A. DE C.V.
CUESTIONARIO DE EVALUACIÓN DE CONOCIMIENTOS SOBRE CIBERSEGURIDAD

Objetivo: identificar el grado de conocimiento que tiene cada uno de los integrantes del encargo de auditoria y colaboradores de la organización en la identificación de posibles ataques cibernéticos a través de la utilización de las tecnologías de la información.

Marque con una "X" en la casilla que considere mas conveniente, en caso sea necesario puede anotar un comentario al respecto.

No.	PREGUNTA	SI	NO	COMENTARIO
1	Al recibir una llamada telefónica, donde se le notifica que es el ganador de un billete de lotería que usted no compro; y que la única condición para poder transferirle el premio es enviar cierta cantidad de dinero a una cuenta bancaria, que se le proporcionara. ¿Usted, aceptaría el acuerdo o que haría en este caso?			
2	¿A su criterio puede la fuga de información confidencial de la entidad repercudir negativamente en su reputación, explique?			
3	Cuando recibe correo electrónico conocidos como basura o Spammers, ¿Usted abre este tipo de correo?			
4	¿Considera usted, que la información procesada haciendo uso de las TIC, está expuesta a riesgos como robo, pérdidas y manipulación por terceros no autorizados? Explique.			
5	¿Tiene usted conocimiento sobre la normativa técnica y legal que trata el tema sobre ciberseguridad?			

6	¿Ha escuchado usted, sobre un incidente sobre robo de información a una prestigiosa empresa a nivel mundial?			
7	¿Considera usted, que la firma de auditoría es susceptible a prácticas de ciberdelincuencia?			
8	¿Alguna vez ha dejado anotaciones de sus credenciales, contraseñas de acceso, entre otros, en lugares visibles? En caso de ser afirmativa su respuesta explique.			
9	¿Considera usted necesario, cambiar sus contraseñas personales o del equipo asignado a su persona, con una frecuencia mínima de dos veces al mes? Explique su respuesta.			
10	¿Ha proporcionado alguna vez, sus credenciales de acceso a compañeros de trabajo o familiares? Explique.			

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

A3

San Salvador, 02 de febrero de 2019

DECLARACIÓN DE CONFIDENCIALIDAD

Señores
AGR Auditores S.A. de C.V.
Presente

Estimados señores,

Para asegurar el continuo cumplimiento con la sección 140 del código de ética emitido por el IESBA relacionados a nuestras responsabilidades profesionales y la protección de nuestros clientes, es esencial que los asuntos de los clientes de la firma permanezcan confidenciales; por lo tanto, declaro mi adscripción a la política de confidencialidad de la firma, bajo los siguientes elementos:

- No divulgaré, ni utilizaré fuera de la firma la información confidencial obtenida en el ejercicio de mis funciones de auditoría dentro de la firma; a menos que exista un requerimiento legal para hacerlo, tales como: orden de la Fiscalía General de la República, por orden de un juez, por orden de la Unidad de Investigación Financiera o cualesquiera otra autoridad judicial que realice investigaciones sobre los clientes de la firma; incluyendo autoridades revisoras del control de calidad, siempre que no se ponga en riesgo la confidencialidad para el cliente.
- Mantendré confidencialidad de los asuntos de los clientes en el entorno no laboral, el cual incluye: conversaciones con otros socios y colegas dentro de la firma, conversaciones fuera de la firma y en el entorno familiar.
- Mantendré confidencialidad de los asuntos que me revelen los potenciales clientes de la firma en los procesos de conocimiento de los mismos.

- En caso de recibir apoyo de otros profesionales, divulgaré la política de confidencialidad y solicitaré a los colaboradores la entrega de un acuerdo de confidencialidad similar.
- Me comprometo en caso de cambiar de trabajo, a no divulgar ninguna información de los clientes, que haya conocido en el desempeño de mis funciones como auditor.

He leído, comprendido, y cumplido con la política de la firma sobre confidencialidad acerca de los asuntos de los clientes de la firma.

Nombre: _____
DUI: _____
Firma: _____

A4

Para: asistente.administrativo1@agrauditores.com.sv

De: soporte@agrauditores.com.sv

Asunto: Correo Phising

Estimados,

Se están recibiendo correos fraudulentos modo phising, que pretende capturar información confidencial de credenciales, por favor eliminar correos de este tipo y por ningún motivo ingresen a los links que se presentan en dichos correos.

Se debe considerar analizar meticulosamente el texto del correo y estar atentos a que pueda tratarse de un engaño. Reportar inmediatamente cualquier actividad sospechosa al departamento de TI.

Gerente de TI

AGR Auditores S.A. de C.V.

A5

Para: asistente.administrativo1@agrauditores.com.sv

De: soporte@agrauditores.com.sv

Asunto: mensaje en cuarentena

Estimados,

Se le informa que ha recibido un correo electrónico, de un usuario desconocido que no pertenece a la red de AGR Auditores S.A. de C.V.; a continuación, se detalla la información contenida en el mensaje:

Fecha/ Hora	**Correo electrónico**
20/11/2019 8:50 a.m.	Czar.morales17@hotmail.com

Acciones a realizar:

Clic en icono → para aceptar el mensaje y poder verlo en su buzón de entrada

Clic en icono ↔ para enviar el mensaje a papelera de reciclaje

Clic en icono !! para enviar todos los mensajes de este usuario a la papelera de reciclaje

AGR Auditores
CRECIENDO CONJUNTAMETE

Gerente de TI

AGR Auditores S.A. de C.V.

A6

Señores de AGR,

Por este medio yo _____ con el cargo _____ empleado de la empresa; declaro que he leído las disposiciones contenidas en las políticas y procedimientos de TI, proporcionadas hacia mi persona por el departamento de recursos humanos el día ____ del mes _____ del año _____.

Firma _____

DUI _____

AGR, S.A. DE C.V.
PROCESOS PARA LA GESTIÓN DE CIBERSEGURIDAD
ÁREA: INTERNET, CONEXIÓN DE DISPOSITIVOS

OBJETIVO GENERAL:
Evaluar la seguridad de internet, conexiones de dispositivos, para determinar la razonabilidad, integridad y confidencialidad. Facilitando a la organización la identificación de posibles ataques cibernéticos a través de la utilización de las tecnologías de la información.

No.	PROCEDIMIENTO	REF.	HECHO POR
1	Definir un protocolo para la identificación, corrección y prevención de vulnerabilidades en las redes y equipos de la organización.		**YRP**
2	Monitorear el uso y actividad de las cuentas de usuario, correo electrónico y del navegador.		**YRP**
3	Implementar protocolos para el uso de dispositivos y servicios externos en la red.		**YRP**
5	Definir el procedimiento a seguir frente a la materialización de un ataque, y el manejo del riesgo reputacional.		**YRP**
6	Verificar que existe control para permitir o denegar el acceso a la Red; y que solamente tenga acceso el personal autorizado.		**YRP**
7	Verificar que existan restricciones a la red WI-FI de la organización, y en caso de encontrarse conectado a la red del cliente, se debe cumplir lo establecido en la política de ciberseguridad de AGR Auditores.		**YRP**
8	Examinar procedimientos para detección de redes y uso compartido.		**YRP**
9	Realizar pruebas de acceso no autorizado y ataques trimestrales, a diferente personal de la organización, para verificar la efectividad de los controles implementados.		**YRP**

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

AGR, S.A. DE C.V
PROCESOS PARA LA GESTIÓN DE CIBERSEGURIDAD
ÁREA: HARDWARE

OBJETIVO GENERAL:

Evaluar el correcto funcionamiento del hardware de la entidad, y su correcta aplicación por parte del personal; detectando vulnerabilidades que permitan mantener actualizadas las medidas de seguridad, por medio de la obtención de evidencia en el desarrollo de cada procedimiento.

No.	PROCEDIMIENTO	REF.	HECHO POR
1	Verifique el cumplimiento de las políticas de compra de tecnología.		**MAG**
2	Constatar que los aparatos de aire acondicionado establecidos en los locales asignados a los servidores de datos funcionen y brinden un ambiente de temperatura adecuado para los equipos informáticos		**MAG**
3	Revisar que se encuentren un kit de herramientas en la entidad para el mantenimiento del hardware		**MAG**
4	Obtener un croquis de la ubicación dentro de la firma del equipo de cómputo en uso		**MAG**
5	Verificar si existe planificación del registro de proveedores de tecnología dentro de la organización.		**MAG**
6	Obtener la verificación de las políticas de mantenimiento en los equipos		**MAG**
7	Las computadoras de todos los servidores poseen su respectivo UPS que ayuda a nivelar el voltaje de las mismas		**MAG**

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

AGR, S.A. DE C.V
PROCESOS PARA LA GESTIÓN DE CIBERSEGURIDAD
ÁREA: REDES

OBJETIVO GENERAL:
Preservar la integridad y confidencialidad de la información compartida por medios conectados entre sí; que permiten continuar con las operaciones del negocio.

No.	PROCEDIMIENTO	REF.	HECHO POR
1	Bloqueo de páginas web clasificadas como no seguras, que pueden representar un riesgo de fuga de información.		**YPR**
2	Bloqueo de acceso al sistema informático, en horas no laborales.		**YPR**
3	Cambio de contraseñas trimestrales que cumplan con lo establecido en la Política de ciberseguridad de la empresa; sobre todo en caso de renuncia de empleados.		**YPR**
4	Bitácora de accesos al sistema informático, sitios web frecuentados por el personal de la empresa.		**YPR**
5	Verificación de cumplimiento de firewall habilitado, y actualización de sistema operativo como navegadores.		**YPR**
6	Revisar que los dispositivos portátiles proporcionados por la firma, solo se han conectado a la red privada de la empresa o autorizadas.		**YPR**
7	Encriptar la comunicación inalámbrica con función WPA2.		**YPR**

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

AGR, S.A. DE C.V.
PROCESOS PARA LA GESTIÓN DE CIBERSEGURIDAD
ÁREA: SOFTWARE

OBJETIVO GENERAL:
Evaluar la correcta aplicación de las actividades de control al software de la entidad, y su correcta aplicación por parte del personal; detectando vulnerabilidades que permitan mantener actualizadas las medidas de seguridad, por medio de la obtención de evidencia en el desarrollo de cada procedimiento.

No.	PROCEDIMIENTO	REF.	HECHO POR
1	Autorizar y verificar periódicamente la instalación de software legal en todos los equipos de la organización. Comprobar adicionalmente que el personal de la organización cumple con la política de evitar descargar software adicional a los ya proporcionados en cada equipo.		**MAG**
2	Implementar y actualizar las configuraciones de seguridad en todos los equipos asignados al personal de la organización. Documentando el proceso mencionado anteriormente y de gestión de cambios.		**MAG**
3	Realizar un seguimiento periódico a la configuración de privilegios tanto en equipos como en programas y redes, actualizándolas de acuerdo al rol de cada colaborador.		**MAG**
4	Verificar la vida útil de las aplicaciones, de tal forma que se actualicen e implementen controles de seguridad.		**MAG**
5	Definir el procedimiento a seguir frente a la materialización de un ataque, y el manejo del riesgo reputacional.	**C1**	**MAG**
6	Realizar pruebas de acceso no autorizado y ataques trimestrales, a diferente personal de la organización, para verificar la efectividad de los controles implementados.		**MAG**

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

C1

AGR, S.A. DE C.V.
GUÍA BÁSICA PARA IDENTIFICACIÓN Y REPORTE DE INCIDENTES DE SEGURIDAD CIBERNÉTICA

Objetivo: Identificar y reporte de incidentes de seguridad cibernética

Tiene como finalidad la gestión de incidentes, su análisis y resolución, para dar una respuesta oportuna por parte del personal de la firma que permitan reducir el riesgo de impacto.

ACTUACIÓN ANTE UN INCIDENTE

Cuando se encuentre ante un incidente de seguridad, se debe procurar recuperar el nivel habitual de funcionamiento de los sistemas o servicios en cuanto a su calidad y disponibilidad, minimizando las pérdidas todo lo posible. A continuación se describen las actuaciones para mitigar los efectos de incidentes de seguridad y recuperar los sistemas afectados, incluyendo un flujograma de las mismas.

RESPUESTAS

1. **Identificación:** en este punto debemos analizar las sospechas sobre posibles anomalías detectadas a través de los controles de seguridad determinados por la organización. Posteriormente se determina el alcance y los sistemas afectados por los incidentes de seguridad cibernética.
2. **Contención y mitigación:** a partir de la información obtenida en el proceso anterior, se debe contener y mitigar lo antes posible, para reducir los riesgos asociados al incidente. Evaluar los equipos afectados, la información que fue vulnerada, entre otros aspectos.
3. **Recuperación:** se deben realizar las anotaciones y documentación soporte sobre el incidente, para poder crear, actualizar medidas de protección que ayuden a combatir similares riesgos en un futuro.

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

C2

AGR, S.A. DE C.V.
LIBRO DE ESTRATEGIAS DE SEGURIDAD

Objetivo: documentar los incidentes cibernéticos que se presenten en las operaciones normales de la firma de auditoría.

Aspectos a considerar.

- Detección de equipos infectados con malware.
- Actividades sospechosas en la red.
- Intentos de autenticación irregulares.
- Intentos de conexión de IP desconocidas.
- Fugas de información.
- Accesos no autorizados a las instalaciones y al sistema.
- Software sin licencia.
- Perdida de hardware.
- Fallos en suministro de servicios básicos (energía eléctrica e internet).
- Equipos desactualizados o en mal estado.

Nota: aquí se debe de incluir cualquier incidente, incluyendo aquellos que no estén detallados anteriormente y que se desarrollen en la firma que comprometan la seguridad de la información.

DETALLE DE INCIDENTES

- **Incidente 1: (describir el incidente)**

Frecuencia con que se presenta:

Fecha del incidente:

Involucrados:

POLITICAS Y PROCEDIMIENTOS

Incidente 1

Procedimientos que se tienen establecidos:

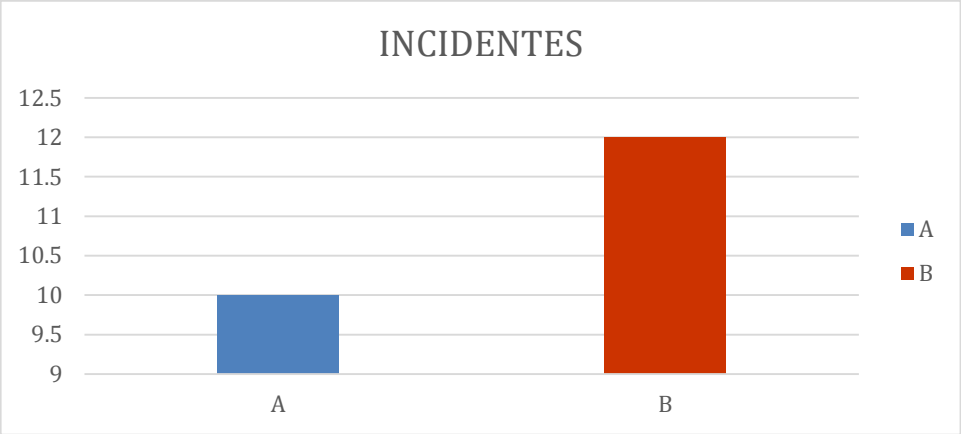
- ✓
- ✓

Procedimientos a implementar después del incidente:

- ✓
- ✓

ESTADISTICAS DE LOS INCIDENTES ANUAL

Etiquetas de fila	Suma de FRECUENCIA
A	10
B	12
Total general	**22**



Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

4.3 *Check list* para el manejo de incidentes de ciberseguridad

Se desarrollará un *check list* para el manejo de incidentes en ciberseguridad, con la finalidad de mostrar las actividades a considerar dentro del control interno para evaluar las acciones a seguir antes, durante y después de un incidente en seguridad. Es importante resaltar que las preguntas no pretenden abarcar todas las situaciones, por lo cual se debe revisar y ajustar a las necesidades de cada organización.

AGR, S.A. DE C.V. **CHECK LIST PARA EL MANEJO DE INCIDENTES DE CIBERSEGURIDAD**		
OBJETIVO GENERAL: Definir actividades para evaluar las acciones a seguir antes, durante y después de un incidente de ciberseguridad, para posteriormente ser incluidas en los procedimientos de control interno dentro de la organización.		
No.	**ACCIÓN**	**RESPUESTA**
1	Realizar una evaluación del impacto ocasionado por la materialización de un incidente de ciberseguridad.	
2	Definir y clasificar los tipos de incidentes de seguridad, asignándole controles y procedimientos de seguridad de acuerdo al daño que ocasionara su materialización.	
3	Integrar un inventario de la información y los recursos más importantes para la operación, de acuerdo con la evaluación de riesgos.	
4	Identificados los responsables de administrar la información y los recursos.	
5	Definir los responsables de gestionar la crisis, en el área legal, de comunicaciones, operaciones y recursos humanos, entre otros.	
6	Documentar los roles y responsabilidades de cada cargo clave responsable de gestionar la crisis	
7	Establecer los umbrales que manejara cada incidente de acuerdo a la calificación de su nivel de riesgo	

8	Mantener una base de datos actualizada, con diferentes números alternos de contacto de los miembros responsables de gestionar la crisis.	
9	Verificar que la organización cuenta con los controles de monitoreo necesarios para proteger y mitigar cualquier fuga de información (antivirus, cortafuegos)	
10	Tener un flujograma de la información que permita identificar los niveles de autoridad para la toma de decisiones ante una crisis.	
11	Capacitar a los colaboradores en la administración y seguridad de la información tanto desde la perspectiva tecnológica como ética.	
12	Preparar a los colaboradores, proveedores y clientes en la identificación y denuncia de acciones sospechas con la información de la organización, así como frente a incumplimientos identificados y niveles de responsabilidad desde cada rol.	
13	Comunicar a la máxima autoridad de la entidad, una descripción de cómo y con quién se está resolviendo el incidente, así como las acciones correctivas frente a la causa raíz.	

Revisado por		**Fecha**		**Firma**	
Autorizado por		**Fecha**		**Firma**	

CONCLUSIONES

La finalidad de la investigación consistió en crear una Guía de Gestión de Riesgos Cibernéticos para empresas dedicadas a brindar servicios de auditoría externa; con el propósito de brindar un ambiente de seguridad y detección oportuna de incidentes de ciberseguridad, llegando a las siguientes conclusiones:

1. La carencia de una gestión efectiva de riesgos cibernéticos en las firmas de auditoría dedicadas a brindar servicios de auditoría externa, se ve reflejado en los resultados; puesto que, se incrementan los desembolsos para solventar incidentes, la imagen de la empresa queda dañada, resulta complicado recuperar la confianza de los clientes, se incurre en procesos judiciales por sustracción de información de terceros no autorizados y en el peor de los casos quiebra del negocio. Por estos motivos, la seguridad cibernética es un componente para el logro de los objetivos de cualquier negocio.
2. Con base en los resultados obtenidos de evaluar la situación actual de la gestión de riesgos cibernéticos, y los recursos que destinan las firmas de auditoría se observa que: a pesar de que las firmas reconocen que existe una alta posibilidad de ser un blanco atractivo para los ciberdelincuentes; es notable la ausencia de medidas, procedimientos y controles en materia de seguridad cibernética; y que si bien se toman ciertas medidas estas no son suficientes o las adecuadas para proteger la información que se trasmite a través del ciberespacio.
3. Las firmas de auditoría carecen de una herramienta robusta para gestionar el riesgo cibernético que les permita garantizar la integridad, confidencialidad y disponibilidad de la información.

RECOMENDACIONES

1. La gestión del riesgo cibernético se vuelve un aspecto importante para mantener el negocio en marcha de la firma de auditoria debido al entorno tecnológico dinámico que continuamente exige adaptación de procesos, debido a lo anterior se debe incorporar en la gestión estratégica de la firma la evaluación del riesgo del ciberespacio, para mantener protegida la información propia y de los clientes.
2. Se recomienda a las firmas de auditoría la creación de un comité de ciberseguridad, que coordine esfuerzos por promover la gestión de riesgos cibernéticos, desde concientizar al personal sobre el impacto negativo, que ocasionaría un incidente de ciberseguridad. Siendo el departamento de informática de las firmas de auditoría, junto al profesional en contaduría, los responsables de la gestión del riesgo; cumpliendo el rol de crear políticas, procedimientos y buenas prácticas en material de ciberseguridad. Puesto que, si la firma de auditoria implementa una serie de medidas o guía para gestionar los riesgos cibernéticos, se le está agregando valor a la entidad.
3. Implementar la guía de gestión de riesgos cibernéticos para las firmas de auditoría, que permita proteger la información de los riesgos y amenazas que surgen cuando se utiliza el ciberespacio de manera que ayude a preservar la integridad, confidencialidad y disponibilidad de la información.

BIBLIOGRAFÍA

Aguilar, L. J. (2017). *Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial.*

Avast. (s.f.). *Malware y antimalware*. Obtenido de Malware y antimalware: https://www.avast.com/es-es/c-malware

Bailón, M. (2012). *Corte interoamericana de derechos humanos.* Obtenido de http://www.corteidh.or.cr/tablas/r28614.pdf

BID. (2016).

Bustos, P., & Araya, M. (2009). *Conociendo las TIC.* Chile. Obtenido de https://l.facebook.com/l.php?u=http%3A%2F%2Frepositorio.uchile.cl%2Fbitstream%2Fhandle%2F2250%2F120281%2FCalandra_Pedro_Conociendo_los_TIC.pdf%3Bsequence%3D1%3Ffbclid%3DIwAR0QM6i1urxFHKrMMK9z1NUDm-_xEJeqj4cwCbKisKgTBA257cGLamczDQc&h=AT2m2Fatvy9An4IcH-Sz9F

Caro, M. (2011). *DIALNET.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/3837251.pdf

CCN. (2015). *Guia de seguridad-glosario y abreviaturas.*

CCN. (2017). *Principios y recomendaciones básicas de seguridad.*

CCN. (2018). *Ciberamenazas y tendencias.*

CCN. (2018). *Medidas de seguridad contra ransomware.*

CCN. (2019). *Criptojacking.*

Centro Criptologico de España (CCN). (2018). *Buenas prácticas en redes sociales.*

CONPES Colombia. (2011). *CONPES 3701*. Colombia. Obtenido de https://www.mintic.gov.co/portal/604/w3-article-3510.html

Digitales, D. (julio de 2018). *Derechos Digitales America Latina*. Obtenido de Derechos Digitales America Latina: https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/?fbclid=IwAR0mWJgRXQVvE5Ll6XWZeIDc0AbGlqCcQR01l3o8QhIrBYzadbe8mtRfgPA

FEPADE, E. E. (2017). Cibercrimen e informática forense: introducción y análisis en El Salvador. *Revista tecnológica N°10*, 66.

Fonseca, B. (02 de Agosto de 2018). *infobae*. Obtenido de infobae: https://www.infobae.com/tecno/2018/08/02/como-prevenir-un-ciberataque-50-mil-millones-de-riesgos-y-enganos-en-solo-82-segundos/

guardian, T. (25 de 2017). *The guardian*. Obtenido de https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

IFAC . (2018). *International Federation of Accountants.* Obtenido de International Federation of Accountants: https://www.ifac.org/publications-resources/new-global-smp-survey-reveals-keys-growth-small-accounting-firms

ISACA. (2019). *ISACA.* Obtenido de ISACA: www.isaca.org

ISO/ IEC 27000. (2018). Gestión de seguridad de la información-visión general y vocabulario.

Molero, X. (2016). *Un viaje a la historia de la informática.* Valencia, España: Universidad Politécnica de valencia. Obtenido de http://museo.inf.upv.es/wp-content/uploads/2016/12/Un%20viaje%20a%20la%20historia%20de%20la%20inform%C3%A1tica.pdf?fbclid=IwAR1BE7gR4gn9Jv6HauU9qaJpU1unKvNEFn8zt0JwY49t_A7fDjzjObyfFls

Organización Internacional de Normalización. (20 de Abril de 2019). *Organización Internacional de Normalización*. Obtenido de Organización Internacional de Normalización: https://www.iso.org

ANEXOS

Anexo 1. Matriz de congruencia.

Grupo N°	S51	**ÁREA:**	Tecnología
Tema aprobado:	“Guía de gestión de riesgos cibernéticos para firmas de auditoría en el área metropolitana de San Salvador”		
Enunciado del problema:	¿En qué medida afecta la ausencia de una guía de gestión de riesgos cibernéticos, para contribuir a la seguridad de la información contenida y manejada en el ciberespacio de las firmas de auditoría en el área metropolitana de San Salvador, y en consecuencia garantizar la confiablidad, integridad y disponibilidad de la misma?		
Objetivo general:	Desarrollar una guía de gestión de riesgos cibernéticos que permita prevenir, proteger, detectar, mitigar y responder ante los principales riesgos a los que están expuestas la firma de auditoría del área metropolitana de San Salvador, El Salvador y generar así un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información.		
Hipótesis:	El diseño y posterior implementación de una guía de gestión de riesgos cibernéticos, contribuirá a mejorar la seguridad de la información contenida y manejada en el ciberespacio; y a garantizar la confiablidad, integridad y disponibilidad de la misma en las firmas de auditoría en el área metropolitana de San Salvador.		

Objetivos específicos	**Unidades de análisis**	**Variable dependiente**	**Variable independiente**	**Indicadores**	**Técnicas a utilizar**	**Tipos de instrumentos a utilizar**
● Evaluar la situación actual de la gestión de riesgos cibernéticos y los recursos que destina las firmas de auditoría del área metropolitana de San Salvador, El Salvador.	Las unidades de análisis para esta investigación son las firmas de auditoría cuyas oficinas están ubicadas en el área metropolitana de San Salvador.	Mejorar la seguridad de la información contenida y manejada en el ciberespacio y a garantizar la confiablidad, integridad y disponibilidad de la misma en las firmas de auditoría en el área metropolitana de San Salvador.	Guía de gestión de riesgos cibernéticos.	VI. Factibilidad de aplicación de procedimientos de gestión de riesgos cibernéticos VI. Conocimiento de leyes y normativa Aplicable	Entrevistas Observación	Anotaciones o notas de campo; bitácora o diario de campo; mapas mentales y fotografías; así como medios audiovisuales, guía de preguntas; susceptibles a cambios en cualquier etapa del estudio.

● Identificar los principales riesgos, amenazas y vulnerabilidad a los que están expuestas firmas de auditoría del área metropolitana de San Salvador, El Salvador como resultado de la interacción entre personas, software, conexión de dispositivos y redes. ● Diseñar una herramienta que permita crear un ambiente de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio para firmas de auditoría del área metropolitana de San Salvador, El Salvador.				VI. Disponibilidad de la administración para la aplicación de la guía de gestión de riesgos cibernéticos V.D Nivel de riesgo aceptado por la administración. V.D Niveles de seguridad alcanzados V.D. Disminución de riesgos VD. Información confidencial, integra y disponible.		

Anexo 2. Glosario

Ciberespacio: es el que resulta de la interacción entre activos físicos y virtuales cuya existencia no es tangible, en él se llevan a cabo actividades de comunicación, comercio e intercambio.

Ingeniería social: consiste en el diseño de mecanismos o esquemas de engaño, destinados a hacer que los usuarios lleven a cabo determinados comportamientos que les van a perjudicar, lo que permite a los cibercriminales obtener un beneficio ilícito; recurre a las pautas conocidas del comportamiento humano que inciten a los usuarios realizar determinadas acciones, accedan a determinados contenidos, proporcionen información en diferentes contextos o compartan datos sensibles. (Centro Criptológico de España (CCN), 2018).

Correos fraudulentos *(phishing)*: es un método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio, mediante campañas de *spam* (correo basura) el atacante puede tratar de engañar al usuario para que descargue y ejecute un programa que supuestamente es legítimo. (CCN, 2019)

Ransomware: "es un código dañino para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado pues el propósito es obtener dinero de manera rápida" (CCN, 2018).

Amenaza: "causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización" (ISO/ IEC 27000, 2018).

Vulnerabilidad: "debilidad de un activo o control que puede ser explotado por una o más amenazas" (ISO/ IEC 27000, 2018).

Ciberataque: "consiste en destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo digital" (ISO/ IEC 27000, 2018).

Ciberdelincuencia: “actividades delictivas llevadas a cabo mediante el empleo del ciberespacio, ya sea para dirigirlas hacia los sistemas y servicios presentes en el mismo o alcanzables a través suyo” (CCN, 2015).

Hacktivismo o ciberactivismo: “activismo digital antisocial. Sus practicantes persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político, o interrumpir servicios, impidiendo o dificultando el uso legítimo de los mismos” (CCN, 2015).

Activo digital: es un recurso controlado de la entidad relacionado con tecnología que poseen valor y del que se esperan obtener beneficios económicos.

Malware: abreviatura de *software* malicioso se considera un tipo molesto o dañino de *software* destinado a acceder a un dispositivo de forma inadvertida, sin el conocimiento del usuario. Los tipos de *malware* incluyen *spyware* (*software* espía), *adware* (*software* publicitario), *phishing*, virus, troyanos, gusanos, *rootkit*, *ransomware* y secuestradores del navegador (Avast).

Rootkit: es un programa diseñado para proporcionar a los hackers acceso administrativo a un equipo sin el conocimiento del usuario (Avast).

Spyware: es un tipo de *malware* difícil de detectar, recopila información sobre hábitos, historial de navegación o información personal (como números de tarjetas de crédito) y a menudo utiliza Internet para enviar esta información a terceros sin el conocimiento del usuario (Avast).

Adware: es un tipo de *software* gratuito patrocinado mediante publicidad que aparece en ventanas emergentes o en una barra de herramientas del equipo o navegador. La mayoría es molesto, pero seguro, algunos se utilizan para recopilar información personal, realizar un seguimiento de los sitios web que visita o incluso registrar las pulsaciones del teclado (Avast).

Secuestradores del navegador: es un programa de *malware* que altera la configuración del navegador del equipo y redirige a sitios web que no tenía intención de visitar y provienen de software de complementos, también conocidos como extensiones del navegador (Avast).

Virus informático: es un programa o un fragmento de código que se carga en el equipo sin conocimiento o permiso, algunos son molestos, pero la mayoría de los virus son destructivos diseñados para infectar y tomar el control de sistemas vulnerables; puede propagarse a través de equipos o redes haciendo copias de sí mismo, del mismo modo que un virus biológico se transmite entre personas (Avast).

Troyano: es un tipo de virus que simula ser algo útil, de ayuda o divertido pero que, de hecho, provoca daños o el robo de datos se propagan a través de un archivo infectado adjunto a un correo electrónico o se esconden tras una descarga de juegos, aplicaciones, películas o tarjetas de felicitación gratuitos (Avast).

Gusanos: "son programas que se autorreplican y se propagan a través de redes de equipos las formas comunes de transmisión de gusanos se incluyen los adjuntos, las redes de intercambio de archivos y los enlaces a sitios web maliciosos" (Avast).

Robo de identidad: consiste en sustraer información personal o de entidades en la que el ladrón se apropia de la identidad de otra persona para realizar actividades como cargos importantes en tarjetas y utilizar nombre e información personal para realizar fraudes.

Gestión de riesgo: consiste en valorar las diferentes medidas de protección y decidir la solución que más se adecue a la entidad (CCN, 2017).

Ataque de día cero: Día cero hace referencia al tiempo que hace que "los buenos" son conscientes de un problema de seguridad del software. Existen dos tipos de día cero. Una vulnerabilidad de día cero es una brecha en la seguridad del software y puede estar en un navegador o en una aplicación. Por otra parte, un

exploit de día cero es un ataque digital que se aprovecha de una vulnerabilidad de día cero para instalar software malicioso en un dispositivo.

Navegar: la acción de visitar páginas del tipo web en la computadora.

Información confidencial: es aquella que no puede ser revelada a terceros sin el consentimiento del titular o dueño de la información.

Riego emergente: es un nuevo peligro identificado, del que pueda ocurrir una exposición significativa en un momento determinado un peligro conocido, del cual pueda ocurrir un inesperado incremento de la exposición.

.

Anexo 3. Entrevista realizada a un gerente de TI

TEMA DE INVESTIGACIÓN: GUIA DE GESTIÓN DE RIESGOS CIBERNÉTICOS PARA LAS FIRMAS DE AUDITORIA EN EL AREA METROPOLITANA DE SAN SALVADOR.

CUESTIONARIO PRE-DISEÑADO PARA ENTREVISTA

Objetivo: Conocer la situación actual de la firma de auditoría respecto al uso del ciberespacio y las medidas de protección de la información.

PARTE I: GENERALIDADES.

Nombre de la firma de auditoría: Elías &Asociados.

Nombre del entrevistado: Héctor Ramírez.

Cargo que desempeña: Gerente de Informática.

PARTE II: CONOCIMIENTO DE LA FIRMA DE AUDITORIA.

1. ¿Mencione usted, cuáles son los servicios que ofrece la organización a sus clientes, y si prestan servicios en línea?

Auditoría financiera, informática, fiscal, gubernamental, capacitación y consultoría gerencial, integral y gestión. Todos los servicios los desarrollamos de forma presencial, ninguno en línea.

2. ¿Mencione cuáles son los tipos de técnicas de mercadeo que utilizan para promocionar sus servicios?

Como firma de auditoría no estamos autorizados a promocionarnos, como firma nos valemos de COMPRASAL para ofrecer nuestros servicios en los diferentes procesos que se publican, y por medio de brindar un servicio de calidad nos permite ser referidos con posibles clientes.

3. ¿Posee la organización página web para promocionar sus servicios? En caso de que la

respuesta sea afirmativa mencionar: Nombre de la página web, y ¿En qué medida contribuye en la obtención de nuevos clientes?

La Firma dispone de un sitio web descriptivo básico, sin embargo, de forma general se pueden describir los servicios brindados.

El acceso a la página de la firma es www.elias.com.sv. Mediante la utilización meta descripciones en las secciones Meta y Title en las páginas web, (palabras claves y frases que las personas probablemente buscarán cuando busquen contenido) logramos que los robots o motores de búsqueda localicen nuestro sitio y se los muestren como alternativa de información a los usuarios. Los resultados de esta técnica son favorables ya que las personas interesadas realizan los contactos, vía correo electrónico o teléfono.

4. ¿Existe un departamento informático o de tecnología? En caso de que la respuesta sea afirmativa mencione sus principales funciones dentro de la organización.

Dentro de la estructura de la firma, se dispone de un departamento de informática que contribuye con el logro de los objetivos de la firma para con sus clientes; inicialmente el departamento fue concebido para brindar soporte técnico preventivo y correctivo al hardware y software utilizado en la firma, entre las actividades que desarrolla el departamento actualmente podemos mencionar las siguientes:

- Soporte técnico preventivo y correctivo a quipo informático.
- Desarrollo y mantenimiento de sitio web.
- Administración de sitio web y cuentas de correo electrónico.
- Desarrollo y mantenimiento de sistemas informáticos internos (contable, facturación, control de planes de pagos, sistema de auditoría Evidenz).
- Mantenimiento de aplicativo web para control de tiempo de empleados en clientes de

auditoría.

- Apoyo de evaluación de controles informáticos en clientes de auditoría financieras.
- Desarrollo de auditorías informáticas.
- Análisis de información de bases de datos de clientes de auditoría.
- Administración de usuarios de red y uso de recursos compartidos en la red (NAS).

PARTE III: TECNOLOGIAS DE LA INFORMACIÓN Y CIBERESPACIO

5. ¿Considera usted, que el uso de las Tecnologías de información y Comunicación (TIC) contribuye al logro de objetivos y metas de la organización? De ser afirmativa su respuesta mencione ejemplos.

En los últimos 15 años el uso de recursos tecnológicos, ha contribuido notablemente en el crecimiento de la firma. Hoy en día todos los empleados disponen de laptops, para el desarrollo de la auditoría y sistema informático de auditoría, que les permiten desarrollar actividades mecanizadas en muy poco tiempo. Sin lugar a duda el uso de recurso tecnológico le ha permitido a la firma un crecimiento sostenible y estable.

6. ¿Se realizan respaldos de la información de la entidad, así como la proporcionada por los clientes? De ser afirmativa su respuesta puede mencionar los medios que se utilizan.

Cada usuario dispone de laptops para el desarrollo del trabajo en los clientes, como medida de seguridad se les recomienda andar únicamente la información del cliente en el que está trabajando, si hay más de un usuario en el cliente se configura una red de trabajo y centraliza la información en un equipo. En la firma, cada usuario dispone de una carpeta con credenciales, las cuales están creadas en un Network Attached Storage (NAS) y únicamente les brinda acceso a los usuarios a los que se les ha brindado permisos. En las carpetas del NAS se guarda toda información de los clientes y de los sistemas, actualmente el NAS dispone de dos discos duros de 2 Tb, en donde se

ha programado que se realicen copias de respaldo en el segundo disco.

Cada 6 meses aproximadamente se realizan respaldos de información en discos duros externos y se mantienen resguardados por los socios en lugares fuera de la oficina.

7. ¿Tiene conocimiento acerca de termino ciberespacio? De ser afirmativa su respuesta Explique un breve concepto y como considera usted, que adentrarse a este mundo mejoraría su negocio.

Podemos considerar el ciberespacio como el entorno artificial que se desarrolla mediante herramientas informáticas. Puede decirse que el ciberespacio es una realidad virtual. No se trata de un ámbito físico, que puede ser tocado, sino que es una construcción digital desarrollada con computadoras. Dicho en palabras más sencillas lo podemos definir como el conjunto de canales de comunicación y medios tecnológicos, que utilizamos para comunicarnos, hacer negocios, promocionarnos, realizar acciones remotas, trasladar información, etc.

Actualmente considero que ya estamos inmersos en el uso del ciberespacio, aunque en una escala mínima, pero a un corto plazo, consideraría que podemos utilizarlo para desarrollar trabajos a distancia, sin la presencia real de empleados, brindar conferencias o realizar ventas.

8. ¿Conoce usted, los tipos de riesgos que existen en el ciberespacio, y en qué manera pueden afectar a su negocio?

Entre los riegos más comunes asociados al ciberespacio podemos mencionar:

- *Spammers*: correo basura, mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- *Scammers:* Se denomina SCAM (o estafa en inglés) a cualquier correo electrónico fraudulento o página web, que pretenda estafar económicamente a cualquier usuario por

medio del engaño.

- *Grooming:* El grooming de niños por Internet (o simplemente grooming) es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un/a adulto/a de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos contra los niños.
- *Sexting:* (contracción de *sex* y *texting*) es un anglicismo de nuevo cuño para referirse al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles.
- *Ciberbullying:* definen comportamientos agresivos practicados a través de muy diferentes dispositivos tecnológicos.

Los negocios pueden afectarse al ser víctimas de robo de información, hackeo de sistemas informáticos y sitios web, hackeo de correos electrónicos, acciones que pueden dañar la imagen de las empresas y con ello la pérdida de confianza de los clientes e incluso tener implicaciones judiciales.

9. ¿Considera usted, que la información procesada haciendo uso de las TIC está expuesta a riesgos de robos, pérdidas y manipulación por terceros no autorizados? Explique.

Con la incorporación de servicios de alojamiento de información en la nube, o simplemente con el uso de correos electrónicos, las posibilidades de robo de información son grandes, es un temor que tiene que ser afrontado por las empresas en nuestro medio, como firma estamos sabedores de estos riesgos.

10. ¿Tiene usted conocimiento sobre el término activos digitales, y si la organización tiene este tipo de activo? Explique.

Si, hoy en día dependemos más de la información digital, (información de clientes, bases de datos, código fuente, informes, papeles de trabajo, contratos, etc.) por tal motivo se ha llegado a considerar que el activo más valioso de toda organización es la información, por ejemplo, código fuente de un sistema informático, podría valer mucho más que el mobiliario y equipo de una empresa.

En el caso de una firma de auditoría, la información que un usuario puede andar en su equipo es muchísimo más valiosa que el mismo equipo en el que la anda, en el caso de un robo de una laptop, esta es sustituida fácilmente, sin embargo, la información puede representar muchísimas horas de trabajo e incluso se puede llegar al incumplimiento de contratos.

11. ¿Considera usted, que la firma de auditoría esta susceptible o expuesta a prácticas de ciberdelincuencia? Explique usted a su criterio, cuál podría ser el impacto que ocasionaría la perdida de información de los clientes.

Todas las empresas que movilizamos algún tipo de información, ya sea propia o de clientes, estamos expuestos al robo de información, chantaje, divulgación o manipulación de datos, en el ciberespacio siempre existirán esos riesgos.

El impacto de perder la información de un cliente, dependerá del nivel de confidencialidad de la información el impacto que ocasionaría podría ser: a) Pérdida de confianza de los clientes para la firma; b) pérdida del cliente; c) Mala reputación de la firma; d) Enjuiciamientos legales por pérdida de información; d) Ser víctimas de cobros por no divulgación de información; e) Ser sancionado por los entes reguladores de auditoría; y el peor de los casos la quiebra de la firma.

PARTE IV: MEDIDAS DE CONTROL INTERNO

12. ¿Tiene conocimiento usted, si se han establecido procedimientos de control que garanticen la seguridad de la información almacenada en las diversas formas de resguardo? Explique.

Se han implementado medidas de seguridad orientadas a la protección de la información, sin embargo, debido al uso y la forma de trabajo siempre se está expuesto a que la información sea extraída por los mismos empleados.

En las instalaciones de la firma, los usuarios tienen acceso restringido tanto físicos como lógicos, sin embargo, la información de los equipos móviles esta siempre expuesta a que pueda ser robada.

Se han implementado medidas como:

- Firma de carta de confidencialidad por parte de los empleados.
- Recomendaciones de andar únicamente la información necesaria en los equipos.
- No extraer información de los clientes en memorias USB.
- Respaldos incrementales del NAS.
- Respaldos de información de sistemas.
- Respaldos de sitio web.
- Uso de correo institucional, etc.

13. ¿Se han establecido políticas de control interno acerca de la seguridad de la información almacenada en el ciberespacio? Si, En caso de ser afirmativa su respuesta mencione: Si se comunican a todo el personal, las actividades de monitoreo que se realizan para verificar su correcto cumplimiento y con qué frecuencia cambian o actualizan las medidas tomadas.

Cada año se firma carta de confidencialidad de la información y durante las juntas de equipo de trabajo se trata de concientizar a los empleados para que hagan buen uso de la información de los clientes sin embargo sabemos que hay mucho que hacer e invertir para tener controlada la información.

PARTE V: USO DE RECURSOS TECNICOS, HUMANOS Y ECONOMICOS.

14. ¿Considera usted, que el personal está capacitado para el uso de las TIC de forma segura?

De ser negativa su respuesta Explique en qué se necesita mejorar.

No, cuando no se dispone de recursos tecnológicos adecuados, para controlar a los empleados lo único que queda es concientizar al buen uso de la información, sin embargo, existen personas que no asumen los riesgos que conlleva la perdida de información tanto para ellos como para la empresa.

Para poder tener mayor control se necesitaría invertir en software y hardware de protección de información, sin embargo, muchas veces las empresas los consideran como gastos debido a los altos costos que representan.

15. ¿Estaría dispuesto a invertir dinero y tiempo en la capacitación de su personal acerca de la ciberseguridad? Si

Héctor Ramírez

Gerente de Informática

Anexo 4. Procesamiento de la información

Categorías y codificación.

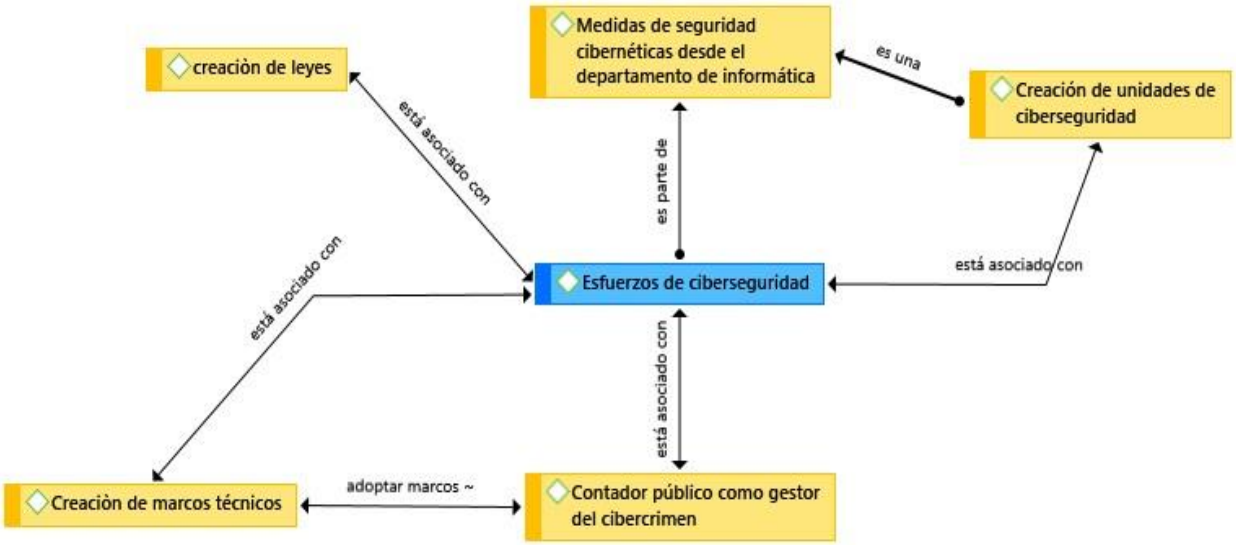


Figura 12. Categoría 1 esfuerzos de ciberseguridad con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

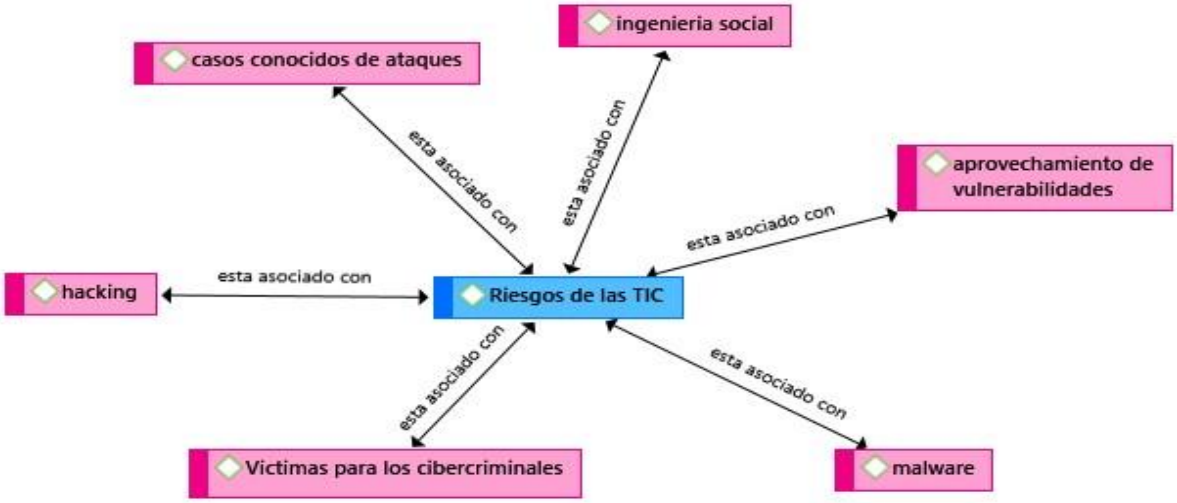


Figura13. Categoría 2 riesgos de las TIC con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

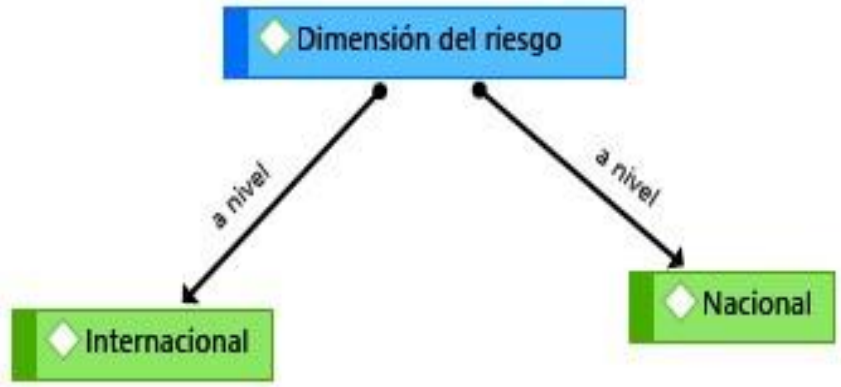


Figura 14. Categoría 3 dimensiones del riesgo con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

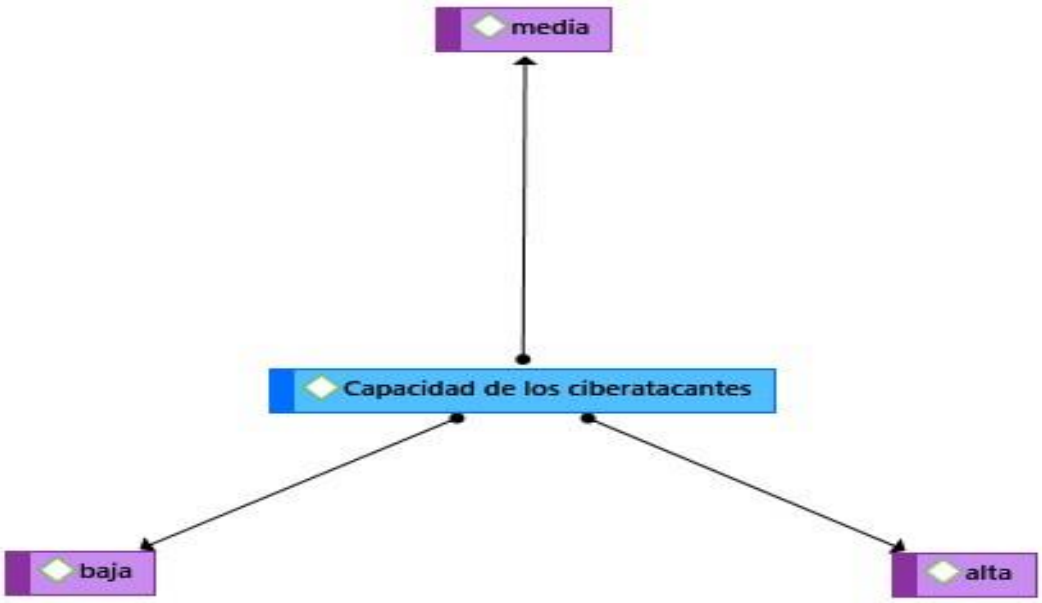


Figura 15. Categoría 4 capacidad de los ciber atacantes con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

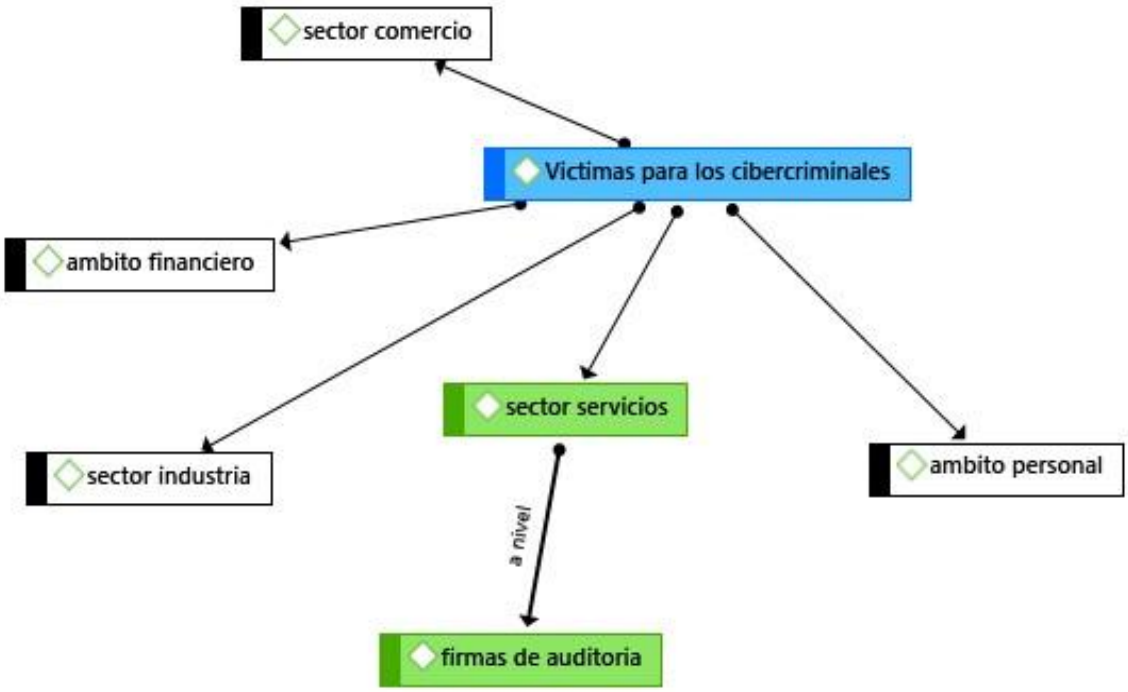


Figura 16. Categoría 5 víctimas para los cibercriminales con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8

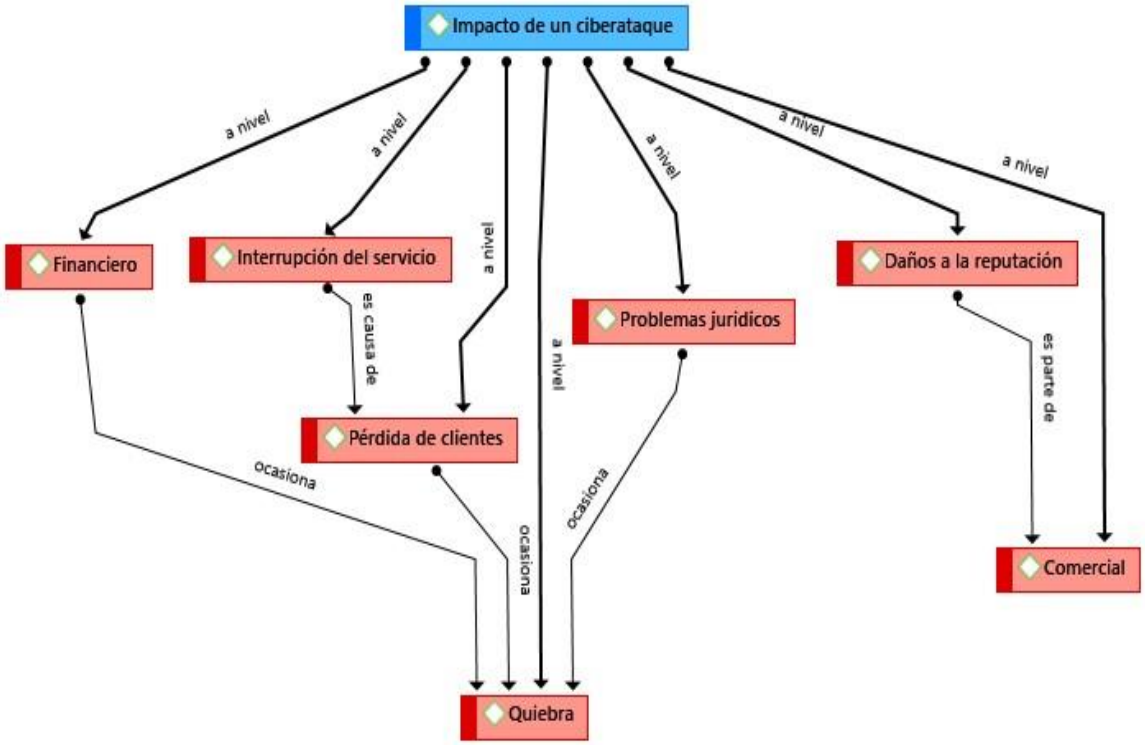


Figura 17. Categoría 6 impacto de un ciberataque con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8

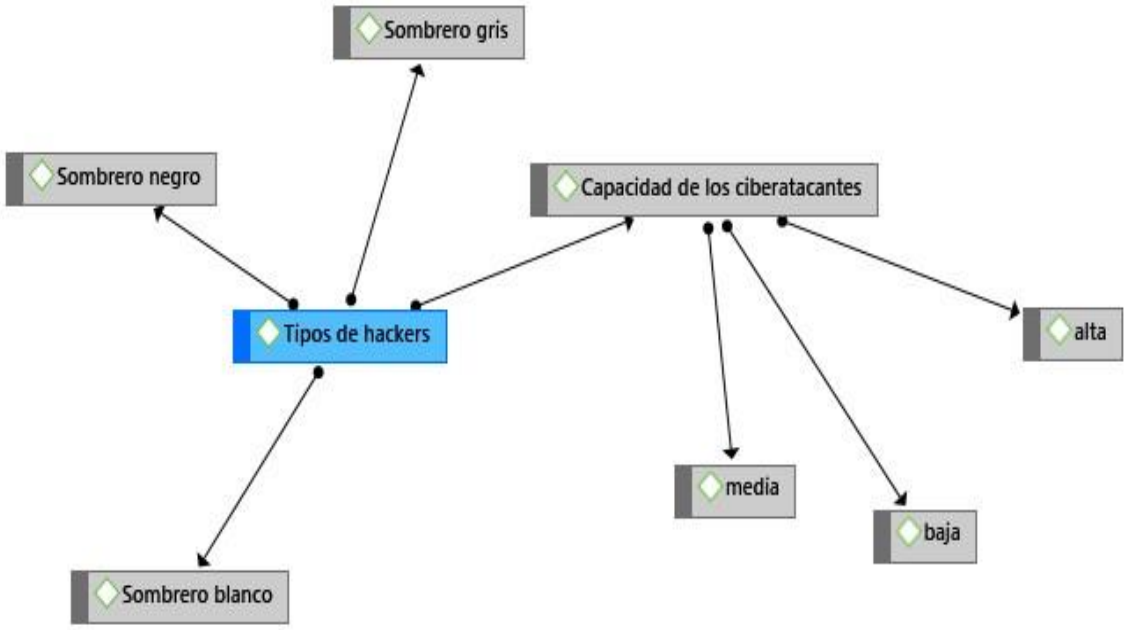


Figura 18. Categoría 7 tipos de hackers con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8

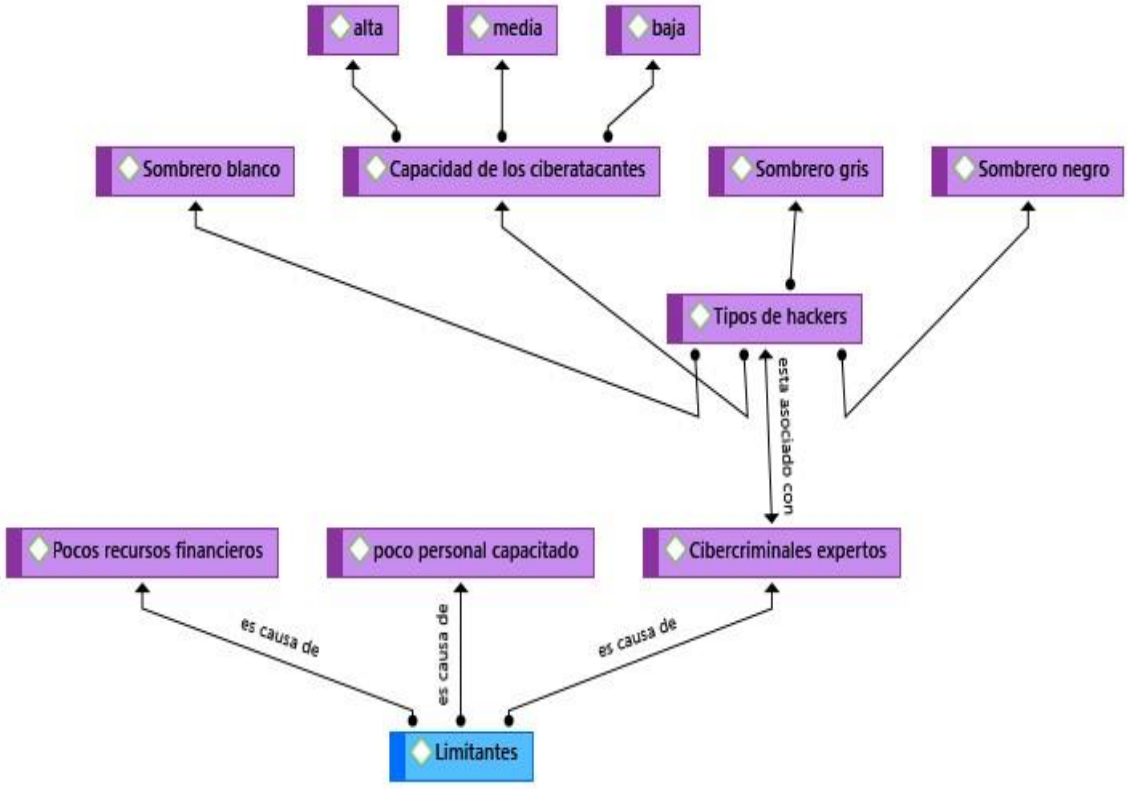


Figura 19. Categoría 8 limitantes con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

Figura 20. Categoría 9 oportunidades con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

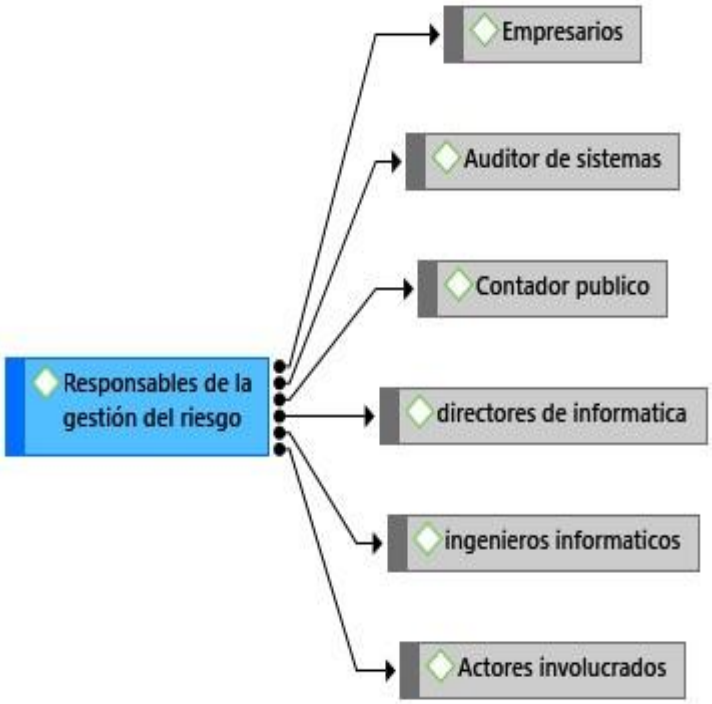


Figura 21. Categoría 10 responsables de la gestión del riesgo con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

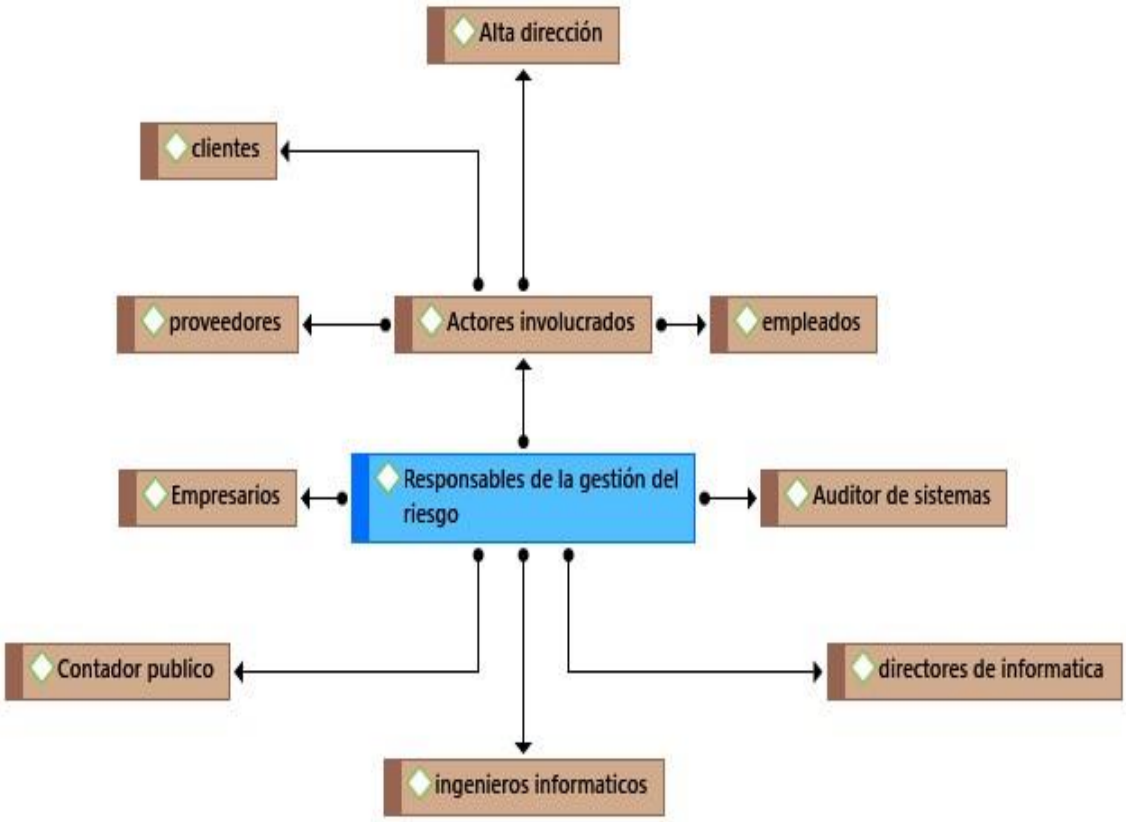


Figura 22. Categoría 11 actores involucrados con los diferentes códigos relacionados. Elaboración propia mediante el software Atlas.ti 8.

Anexo 5. Análisis e interpretación de los datos procesados

a) Información recopilada de la entrevista

Entrevista realizada a un gerente de TI- pregunta X: **ERGTI-PX**

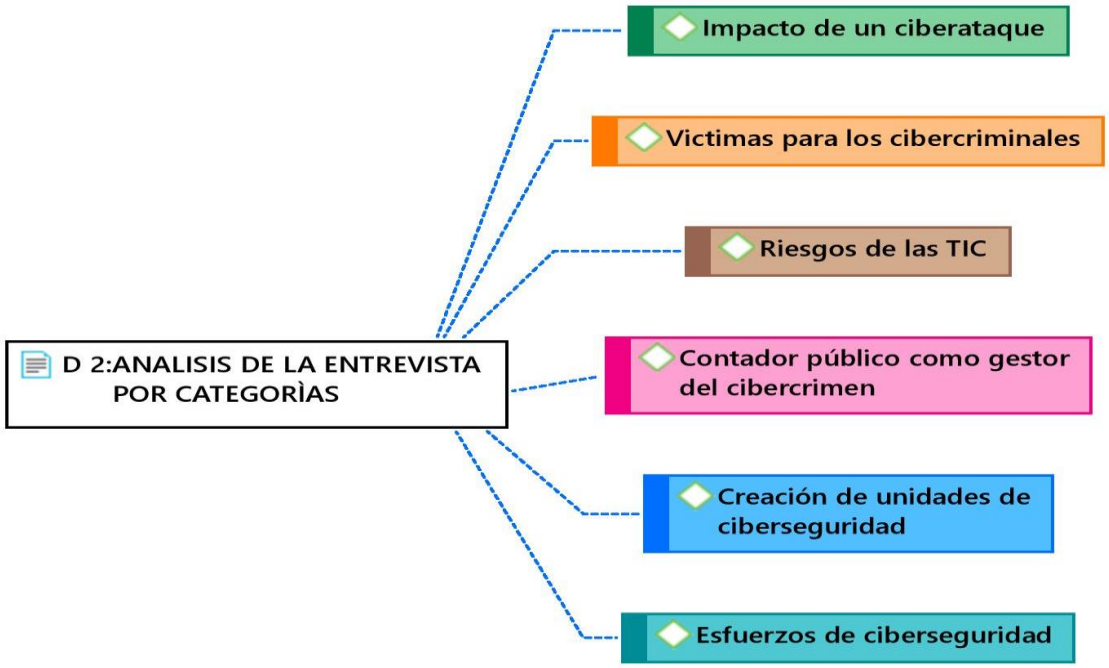


Figura 23. Análisis de entrevista por categorías, elaboración propia mediante el uso del software Atlas.ti 8.

Categoría 1. Esfuerzos de ciberseguridad a nivel mundial (ver figura 9)

- **Creación de unidades de ciberseguridad en las entidades o firmas de auditoria**

En cuanto a la categoría 1 se obtuvo la siguiente manifestación como resultado de la entrevista.

Dentro de la estructura de la firma, se dispone de un departamento de informática que contribuye con el logro de los objetivos de la firma para con sus clientes; inicialmente el departamento fue concebido para brindar soporte técnico preventivo y correctivo al hardware y software utilizado en la firma, entre las actividades que desarrolla el departamento actualmente podemos mencionar las siguientes:

- Soporte técnico preventivo y correctivo a quipo informático.

- Desarrollo y mantenimiento de sitio web.
- […], véase anexo 3. **ERGTI-P4**

Entre los elementos que surgen se pueden mencionar:

No existe una actividad explicita del departamento que se enfoque en ciberseguridad, encontrándose por lo tanto carencias en el objetivo de la unidad.

- **Contador público como gestor del cibercrimen en las firmas de auditoría.**

Para el análisis de este indicador en cuanto a la categoría 1 se han seleccionado las siguientes manifestaciones de la **ERGTI.**

- Auditoría Financiera.
- Auditoría Fiscal.
- Auditoría Gubernamental.
- Auditoría y Consultoría Integral y Gestión.
- Auditoría Informática.
- […], véase anexo 3. **ERGTI-P1**

La firma de auditoría no brinda servicios relacionados con ciberseguridad, lo que debe alertarle a que están surgiendo nuevas formas de hacer negocios (en un entorno cibernético, para el caso) y con ello debe de estar preparada no solo para resguardar su información, sino, para ofrecer sus servicios de gestión de seguridad cibernéticas a terceros.

Por lo tanto, debe poseer profesionales que estén capacitados y aptos para atender y gestionar sucesos derivados de las actividades cibernéticas.

No, cuando no se dispone de recursos tecnológicos adecuados, para controlar a los empleados lo único que queda es concientizar al buen uso de la información, sin embargo, existen personas que no asumen los riesgos que conlleva la perdida de información tanto para ellos como para la

empresa. Véase anexo 3. **ERGTI-P14**

Es notorio que la firma de auditoría carece en general de personal con la suficiente capacitación en el uso de las TIC de forma segura, lo que a futuro puede traer diversidad de riesgos a la empresa. Así mismo el personal de la firma de auditoría posee limitantes para gestionar un riesgo cibernético.

- **Medidas de seguridad cibernéticas desde el departamento de informática de la entidad, si se posee.**

Al abordar sobre las medidas en materia de ciberseguridad obtuvimos las siguientes respuestas:

Si, se comunican a todo el personal, las actividades de monitoreo que se realizan para verificar su correcto cumplimiento y con qué frecuencia cambian o actualizan las medidas tomadas.

Cada año se firma carta de confidencialidad de la información y durante las juntas de equipo de trabajo se trata de concientizar a los empleados para que hagan buen uso de la información de los clientes sin embargo sabemos que hay mucho que hacer e invertir para tener controlada la información. Véase anexo 3. **ERGTI-P13**

Se han implementado medidas de seguridad orientadas a la protección de la información, sin embargo, debido al uso y la forma de trabajo siempre se está expuesto a que la información sea extraída por los mismos empleados.

En las instalaciones de la firma, los usuarios tienen acceso restringido tanto físicos como lógicos, sin embargo, la información de los equipos móviles esta siempre expuesta a que pueda ser robada. Véase anexo 3. **ERGTI-P12**

Al analizar las respuestas a las preguntas 12 y 13 de la **ERGIT** se reconoce la ausencia de medidas claras en materia de seguridad cibernética. Y se resalta la demostración de sinceridad y transparencia al reconocer que si bien se toman ciertas medidas estas no son suficientes o las

adecuadas. Es de tener claro que, aunque hubiera mejores medidas estas no garantizan a un cien por ciento evitar eventos desafortunados.

Categoría 2. Riesgos de las TIC (ver figura 10)

Para categoría se identificaron sub categorías definiendo una serie de riesgos que se analizarán a partir de las manifestaciones obtenidas de la entrevista al gerente de IT.

Sub categorías:

e) *Malware, b) a*provechamiento de vulnerabilidades, c) ingeniería social y d) h*aking.*

Las manifestaciones del gerente de IT fueron:

Entre los riegos más comunes asociados al ciberespacio podemos mencionar:

- *Spammers:* correo basura, mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- *Scammers:* Se denomina SCAM (o estafa en inglés) a cualquier correo electrónico fraudulento o página web, que pretenda estafar económicamente a cualquier usuario por medio del engaño.
- *Ciberbullying:* definen comportamientos agresivos practicados a través de muy diferentes dispositivos tecnológicos.
- […]

Los negocios pueden afectarse al ser víctimas de robo de información, hackeo de sistemas informáticos y sitios web, hackeo de correos electrónicos, acciones que pueden dañar la imagen de las empresas y con ello la pérdida de confianza de los clientes e incluso tener implicaciones judiciales. Véase anexo 3. **ERGTI-P8**

Con la incorporación de servicios de alojamiento de información en la nube, o simplemente

con el uso de correos electrónicos, las posibilidades de robo de información son grandes, es un temor que tiene que ser afrontado por las empresas en nuestro medio, como firma estamos sabedores de estos riesgos. Véase anexo 3. **ERGTI-P9**

Actualmente considero que ya estamos inmersos en el uso del ciberespacio, aunque en una escala mínima, pero a un corto plazo, consideraría que podemos utilizarlo para desarrollar trabajos a distancia, sin la presencia real de empleados, brindar conferencias o realizar ventas. Véase anexo 3. **ERGTI-P7**

En lo que se refiere a riesgo de las TIC se detecta que se tiene claro que en algún momento de una u otra forma puede adentrarse a este mundo virtual (ciberespacio) y esto trae consigo la existencia de riesgos a los cuales puede estar expuesta.

Además, según lo manifestado en la respuesta a la P-8 de ERGTI expresa el conocimiento de cuáles son los principales riesgos a los cuales la firma está expuesta.

Categoría 5. Impacto de un ciberataque. (Ver figura 14)

En la categoría nos interesa saber si existe la conciencia del impacto que pudiera tener sobre la firma de auditoría un posible ataque cibernético.

Las subcategorías en general son las siguientes:

a) Financiero, b) comercial, c) daños en la reputación, d) problemas jurídicos, e) pérdida de clientes, f) quiebra, g) interrupción de servicios y h) atrasos.

El análisis a esta categoría se realiza a través de las siguientes manifestaciones:

Todas las empresas que movilizamos algún tipo de información, ya sea propia o de clientes, estamos expuestos al robo de información, chantaje, divulgación o manipulación de datos, en el ciberespacio siempre existirán esos riesgos.

El impacto de perder la información de un cliente, dependerá del nivel de confidencialidad de la

información el impacto que ocasionaría podría ser:

- Pérdida de confianza de los clientes para la firma.
- Mala reputación de la firma.
- Enjuiciamientos legales por pérdida de información.
- Ser víctimas de cobros por no divulgación de información.
- Ser sancionado por los entes reguladores de auditoría y el peor de los casos la quiebra.

De lo anterior se destaca que no solo se tiene conciencia de que existen posibles riesgos a los que se pueden estar expuestos como lo tratado en el análisis de la **categoría 2 riesgo de las TIC,** sino que la firma tiene una idea a manera general del impacto de lo que la ocurrencia de los riesgos pudiera generar.

Categoría 5. Víctimas para cibercriminales. (ver figura 13)

Sub categorías relacionadas

a) sector servicios y b) firmas de auditoría

Se realiza una relación entre las firmas de auditoría y el sector servicios al cual pertenecen y se cruzan las manifestaciones de la **ERGTI-P3; ERGTI-P7; ERGTI-P9; ERGTI-P10; Y ERGTI-P11.** Véase anexo 3.

La Firma dispone de un sitio web descriptivo básico, sin embargo, de forma general se pueden describir los servicios brindados. **ERGTI-P3**

Actualmente considero que ya estamos inmersos en el uso del ciberespacio, aunque en una escala mínima, pero a un corto plazo, consideraría que podemos utilizarlo para desarrollar trabajos a distancia, sin la presencia real de empleados, brindar conferencias o realizar ventas. **ERGTI-P7**

Con la incorporación de servicios de alojamiento de información en la nube, o simplemente con el uso de correos electrónicos, las posibilidades de robo de información son grandes, es un

temor que tiene que ser afrontado por las empresas en nuestro medio, como firma estamos sabedores de estos riesgos. **ERGTI-P9**

Si, hoy en día dependemos más de la información digital, (información de clientes, bases de datos, código fuente, informes, papeles de trabajo, contratos, etc.) por tal motivo se ha llegado a considerar que el activo más valioso de toda organización es la información, por ejemplo, código fuente de un sistema informático, podría valer mucho más que el mobiliario y equipo de una empresa.

En el caso de una firma de auditoría, la información que un usuario puede andar en su equipo es muchísimo más valiosa que el mismo equipo en el que la anda… **ERGTI-P10**

Todas las empresas que movilizamos algún tipo de información, ya sea propia o de clientes, estamos expuestos al robo de información, chantaje, divulgación o manipulación de datos, en el ciberespacio siempre existirán esos riesgos. **ERGTI-P11**

La firma de auditoría forma parte de usuarios que una u otra forma se puede convertir en blanco de cibercriminales. La firma de auditoría manifiesta el hecho de que ya está inmersa en este mundo virtual y que por lo tanto está expuesta a hechos como los mencionados en **ERGTI-P11.**

Por lo tanto, a partir de lo anterior podemos observar que existe conciencia por parte de la firma que en algún momento este o no totalmente inmerso en un mundo digital (ciberespacio) será un blanco para delincuentes.

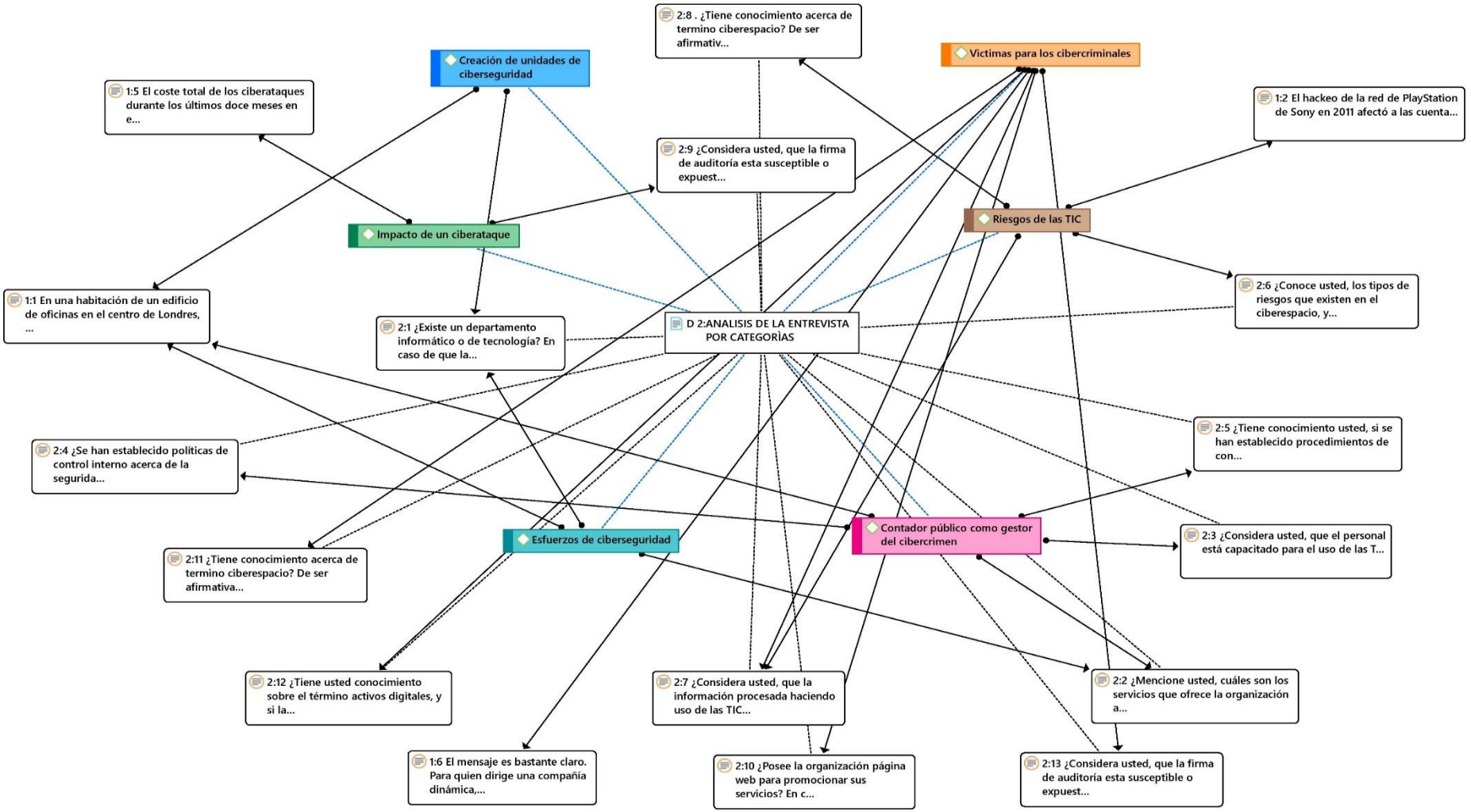


Figura 24. Análisis de entrevista por categorías, elaboración propia mediante el uso del software Atlas.ti 8.

b) Aporte de lecturas y textos

Analizaremos los textos recopilados con el mismo seguimiento de categorías y subcategorías dado a la entrevista. Emitiendo un breve comentario.

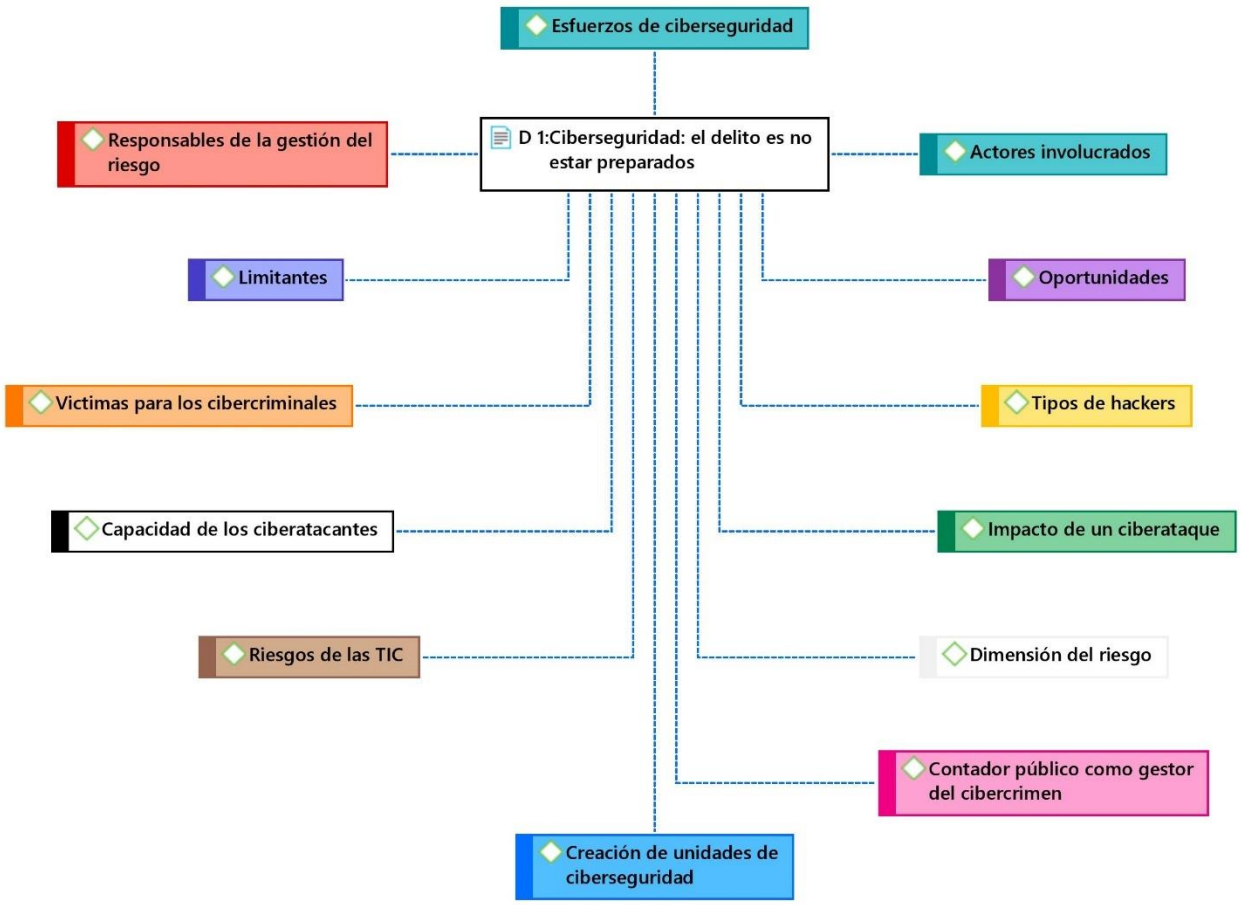


Figura 25. Análisis de entrevista por categorías, elaboración propia mediante el uso del software Atlas.ti 8.

1. Esfuerzos de ciberseguridad a nivel mundial (ver figura 9)

- **Creación de marcos técnicos para la gestión del cibercrimen**

En una habitación de un edificio de oficinas en el centro de Londres, un grupo de personas se dedica a encontrar brechas en las defensas cibernéticas de empresas y organizaciones. Hay muchas habitaciones así en todo el mundo, pero a diferencia de la mayoría, ésta la controlan los buenos. (Grant Thornton Corporación S.L.P., 2016)

Es evidente que existe la necesidad de directrices y buenas prácticas que nos preparen para afrontar este

nuevo mundo virtual llamado ciberespacio y no solo nos preparen, sino que nos protejan ante actuaciones que violen derechos fundamentales.

2. Riesgos de las TIC (ver figura 10)

- Haking

"El hackeo de red a PlayStation de Sony en 2011, afectó las cuentas de 77 millones de usuarios. Una cifra que se vio eclipsada por el ataque a Yahoo que comprometió los datos de 500 millones de personas en 2014". (Grant Thornton Corporación S.L.P., 2016)

Todas las empresas no importando su tamaño están expuestas a riesgos y de ocurrir un evento como en los ejemplos anteriores no solo se puede ver afectada la empresa sino una gran cantidad de usuarios internos o externos.

3. Dimensión del riesgo. (ver figura 11)

- Nacional
- Internacional

Según el último International Business Report de Grant Thornton, una encuesta a 2.500 líderes empresariales en 36 economías de todo el mundo, la ciber extorsión está particularmente extendida en Asia y Latinoamérica, especialmente en el sector de servicios.

No importa si se está en un país desarrollado o no, si la empresa está asentada en un país con poder económico o está en uno no tan favorable, los ataques son reales y pueden ocurrir en cualquier momento y cualquier empresa puede estar expuesta a estos, sea cual sea el rubro al que se dedique. Ahora es de sumo interés para las firmas de auditoría prestar atención al hecho de que los ataques están ocurriendo en una mayor medida sobre el sector servicio.

4. Capacidad de los ciber atacantes. (ver figura 12)

- Alta
- Media

- Baja

Otra conclusión derivada del IBR es que las ciber amenazas ya no provienen exclusivamente de los dormitorios de geeks adolescentes, sino que se han convertido en una enorme industria global.

Con el crecimiento de la tecnología las amenazas y riesgos se vuelven más sofisticadas y los ciber atacantes buscan ya no solo diversión si no que beneficios económicos y daños a la imagen comercial de la entidad por los que podemos relacionar con la categoría de impacto de un ciberataque (ver figura 14).

En la firma de auditoria se tiene claro que la incorporación de servicios de alojamiento de información en la nube, o simplemente con el uso de correos electrónicos, las posibilidades de robo de información son grandes, es un temor que tiene que ser afrontado por las empresas en nuestro medio, como firma estamos sabedores de estos riesgos. **ERGTI-P11.**

5. **Impacto de un ciberataque. (ver figura 14)**

- Financiero
- Comercial
- Daños en la reputación
- Problemas jurídicos
- Pérdida de clientes
- Quiebra
- Interrupción de servicios
- Atrasos

El coste total de los ciberataques durante el año 2016 se estima en unos 265.000 millones, y ha aumentado respecto al año anterior.

Pero las pérdidas financieras no son el principal impacto que destacan las empresas afectadas por los ciberataques. La pérdida de reputación, el tiempo invertido en gestionarlos, la consiguiente pérdida de clientes y los costes de implementar defensas adecuadas son considerados como más importantes que la pérdida directa de facturación.

En la firma de auditoria se tiene claro pues en la respuesta obtenida se hace una manifestación de los riesgos a los que está expuesta la información.

(...) Los negocios pueden afectarse al ser víctimas de robo de información, hackeo de sistemas informáticos y sitios web, hackeo de correos electrónicos, acciones que pueden dañar la imagen de las empresas y con ello la pérdida de confianza de los clientes e incluso tener implicaciones judiciales. **ERGTI-P8.**

Con la incorporación de servicios de alojamiento de información en la nube, o simplemente con el uso de correos electrónicos, las posibilidades de robo de información son grandes, es un temor que tiene que ser afrontado por las empresas en nuestro medio, como firma estamos sabedores de estos riesgos. **ERGTI-P9.**

Al realizar un análisis más profundo se identifica que la firma de auditoria tiene claro el impacto de un ciberataque sin embargo las medidas implementadas con son lo suficiente fuertes para garantizar la integridad confidencialidad de la información según la siguiente respuesta:

Se han implementado medidas de seguridad orientadas a la protección de la información, sin embargo, debido al uso y la forma de trabajo siempre se está expuesta a que la información sea extraída por los mismos empleados.

En las instalaciones de la firma, los usuarios tienen acceso restringido tanto físicos como lógicos, sin embargo, la información de los equipos móviles esta siempre expuesta a que pueda ser robada. Se han implementado medidas como:

- Firma de carta de confidencialidad por parte de los empleados.
- Recomendaciones de andar únicamente la información necesaria en los equipos.
- No extraer información de los clientes en memorias USB.
- Respaldos incrementales del NAS.
- Respaldos de información de sistemas.
- Respaldos de sitio web.
- Uso de correo institucional, etc. **ERGTI-P12.**

6. Victimas para cibercriminales. (ver figura 13)

- Sector comercio
- Sector servicios
- Firmas de auditoría
- Sector industrial
- Sector financiero
- Datos personales

El mensaje es bastante claro. Para quien dirige una compañía dinámica, estar preocupado de manera casi obsesiva por la seguridad no es un síntoma de paranoia. Alguien, en algún lugar, está detrás de su empresa. Pueden ser *"hacktivistas*" en pos de lo que consideran una agenda ética, cibercriminales al servicio de las mafias, hackers patrocinados por estados o terroristas. Que una compañía se convierta en objetivo de estos grupos es sólo cuestión de tiempo, si es que no ha ocurrido ya.

Las firmas de auditoría se encuentran en el sector servicios y manejan una gran cantidad de información.

Todas las empresas que movilizamos algún tipo de información, ya sea propia o de clientes, estamos expuestos al robo de información, chantaje, divulgación o manipulación de datos, en el ciberespacio siempre existirán esos riesgos. **ERGTI-P11.**

7. Tipos de hacker. (ver figura 15)

- Sombrero blanco
- Sombrero gris
- Sombrero negro

¿Cómo pueden empezar las organizaciones a combatir estas amenazas? Nick Smith, jefe de pruebas de incursión en Grant Thornton UK, es lo que se conoce como un hacker ético. Como experto en informática, se dedica a intentar asaltar los sistemas y redes de sus clientes con el fin de encontrar vulnerabilidades que pudieran ser explotadas por un hacker malicioso.

Existen diferentes tipos de hackers unos buscan vulnerabilidad para entidades para luego darlas a conocer y estas se solventen sin embargo otros buscan beneficios diversos entre los que se puede mencionar obtención de beneficios económicos.

La firma tiene claro que pueden ser víctimas de hackeos tal como lo manifiestan

(...) Los negocios pueden afectarse al ser víctimas de robo de información, hackeo de sistemas informáticos y sitios web, hackeo de correos electrónicos, acciones que pueden dañar la imagen de las empresas y con ello la pérdida de confianza de los clientes e incluso tener implicaciones judiciales. **ERGTI-P11.**

8. Limitantes. (ver figura 16)

- Pocos recursos financieros
- Poco personal capacitado
- Cibercriminales expertos

Para Smith, “nuestro trabajo no es hacer su red impenetrable, eso es sencillamente imposible. Tenemos muchas capacidades, pero no la ingente cantidad de personas y dinero con la que a veces nos enfrentamos. Además, siempre habrá alguien que encontrará un nuevo método para atacar a las organizaciones.

El recurso humano es capaz de aprender si se le instruye y facilitan las herramientas, pero en ocasiones no se cuentan con recursos suficientes para invertir.

En la firma de auditoria conocen sus limitantes tal como lo expresan:

Cuando no se dispone de recursos tecnológicos adecuados, para controlar a los empleados lo único que queda es concientizar al buen uso de la información, sin embargo, existen personas que no asumen los riesgos que conlleva la perdida de información tanto para ellos como para la empresa.

Para poder tener mayor control se necesitaría invertir en software y hardware de protección de información, sin embargo, muchas veces las empresas los consideran como gastos debido a los altos costos que representan. **ERGTI-P14.**

Pero al preguntar si están dispuestos a invertir para gestionar el riesgo que implica el uso del ciberespacio la respuesta es afirmativa. **ERGTI-P15.**

9. Oportunidades (ver figura 17)

- Creación de políticas
- Creación de procedimientos
- Adopción de buenas practicas

Lo que hacemos es pasar a la ofensiva y encontrar todos los fallos de seguridad que podamos. A partir de ello redactamos nuestro informe con medidas prácticas para que las organizaciones puedan estar tan seguras como sea posible.”

Los informes y guías de buenas prácticas de ciberseguridad son una herramienta muy útil y efectiva para gestionar el riesgo del ciberespacio, si en una organización se crean una serie de medidas o guía para gestionar este tipo de riesgo se está agregando valor a la entidad y ayudando a preservar la integridad, confidencialidad y disponibilidad de la información.

10. Responsables de gestión del riesgo (ver figura 18)

- Directores de informática
- Ingenieros informáticos
- Empresarios
- Contador publico
- Auditor

"No todo el mundo se da cuenta de lo fácil que resulta acceder a ordenadores, dispositivos móviles y redes y de los enormes riesgos que esto conlleva. Ya no es un tema que incumba únicamente a los directores de informática."

La dimensión del riesgo que implica la interacción en el ciberespacio es nacional e internacional y los responsables de la gestión ya no son solo los profesionales de informática o ingenieros si no que es un tema que incluye al profesional de la contaduría pública como auditor y gestor de riesgo de manera que se agregue valor a la entidad por medio de la protección de la información almacenada en el ciberespacio.

11. Actores que intervienen (ver figura 19)

- Alta dirección
- Empleados de las entidades
- Clientes
- Proveedores

La ciberseguridad tiene que estar en la agenda de toda la alta dirección y requiere un enfoque que abarque a toda la compañía. Cuanto más se retrase la respuesta más aumenta la amenaza. Las organizaciones tienen que actuar ya.

Es importante que todos los miembros de la firma de auditoria tengan conocimientos acerca de los riesgos del ciberespacio y como gestionarlos pues la labor de un profesional de la contabilidad y auditoría se vería limitada si los demás actores no propician un ambiente de cooperación para la protección de la información.

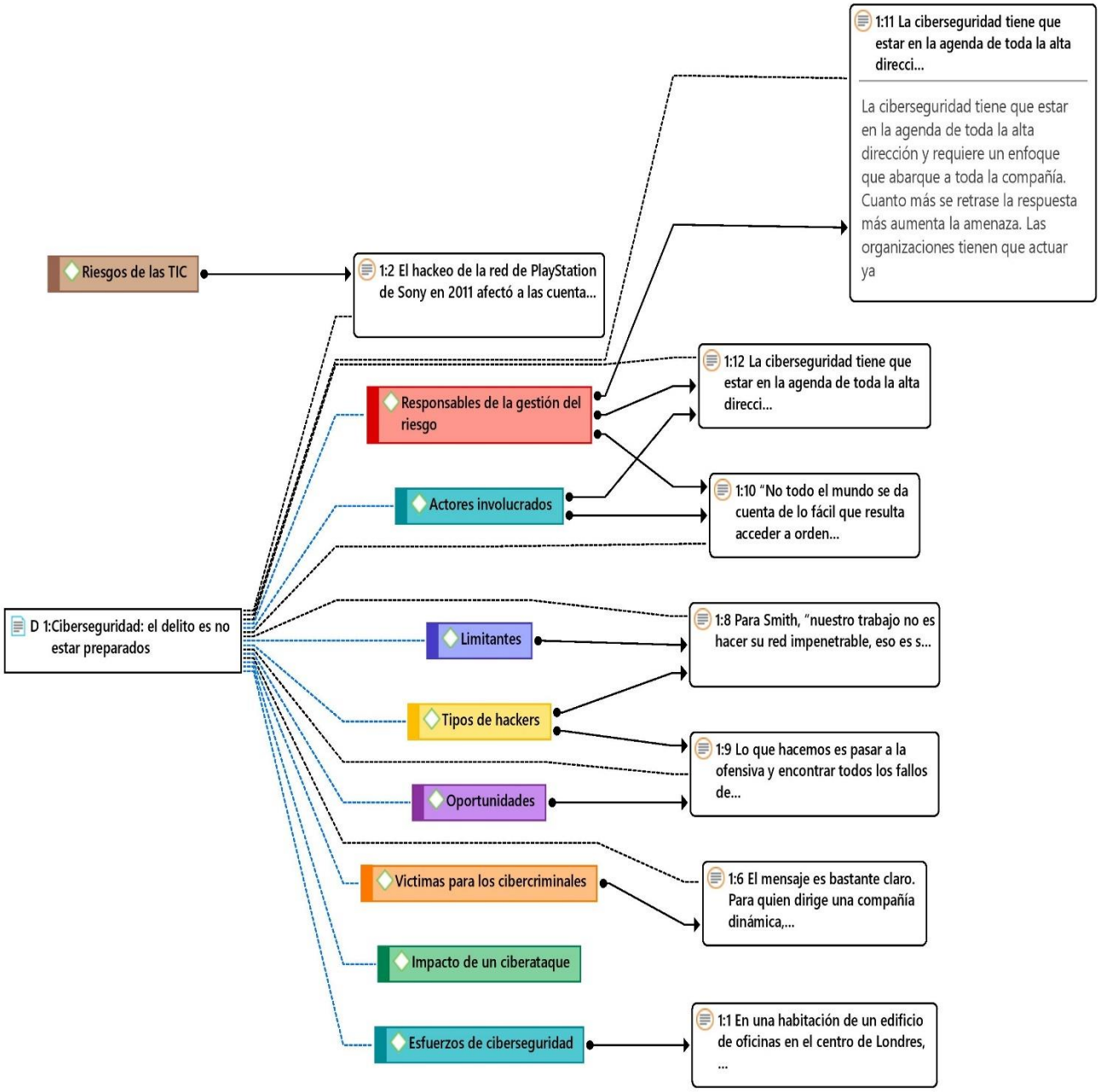


Figura 26. Análisis de entrevista por categorías, elaboración propia mediante el uso del software Atlas.ti 8.