El Revisor Fiscal y la Ciberseguridad en tiempos de pandemia

Dayana Lisneth Hayde Do Santos

Universidad Militar “Nueva Granada”

Facultad Ciencias Económicas

Especialización en Revisoría Fiscal y Auditoría Internacional

Bogotá D.C. 2021

Tabla de Contenido

Lista de Figuras

Lista de tablas

Resumen

Los delitos informáticos han crecido exponencialmente debido al cambio de modo presencial al virtual, permitiéndoles a los criminales la posibilidad de cometer este delito. Por su parte el revisor fiscal maneja una gran cantidad de información, pero conocen y aplican alguna herramienta que permita fortalecer la seguridad de la información, para reducir la posibilidad de las organizaciones ser víctimas de este tipo de delito. Este ensayo fue basado en el estudio de investigación de tipo descriptivo puesto que describe los delitos informáticos, la ciberseguridad y el revisor fiscal y como se relacionan. La metodología utilizada es de tipo exploratoria ya que busca tratar un tema que no ha sido analizado y que prácticamente hay poca información sobre ella en conjunto.

Palabras clave: Ciberseguridad, delitos informáticos, revisor fiscal, programas académicos.

Abstract

Computer crimes have grown exponentially due to the change from face-to-face to virtual mode, allowing criminals the possibility of committing this crime. For his part, the tax auditor handles a large amount of information, but they know and apply some tool that allows strengthening information security, to reduce the possibility of organizations being victims of this type of crime. This essay was based on a descriptive research study since it describes cybercrime, cybersecurity and the tax auditor and how they are related. The methodology used is exploratory as it seeks to address a topic that has not been analyzed and that there is practically little information on it as a whole.

Keywords: Cybersecurity, computer crime, tax auditor, academic programs

Introducción

El Revisor Fiscal, como parte de su trabajo, maneja una gran cantidad de información, que por consiguiente tiene la finalidad de apoyar su plan de trabajo, es así que existe la pregunta, si el revisor utiliza o tiene conocimiento sobre alguna herramienta que le proporcione seguridad sobre la información que posee. Ya que en estos ultimo años, o desde que comenzó la pandemia por Covid-19, los delitos informáticos han aumentado drásticamente debido al cambio de modo virtual. No muchos conocen, y que pocos aplican, es la ciberseguridad, donde este a través de un conjunto de herramientas y procedimientos protege la información generada y procesada a través de la tecnología.

El crecimiento de los delitos informáticos afecta de por sí a todo el mundo, sin embargo, las empresas son víctimas de estos criminales más a menudo puesto que ellos manejan demasiada información que podría para ellos ser una llave para su economía. Y el revisor fiscal podría tomar un papel importante para poder reducir la posibilidad de que las entidades sean víctima de este tipo de delito.

La metodología utilizada es de tipo exploratoria ya que busca tratar un tema que no ha sido analizado y que prácticamente hay poca información sobre ella en conjunto, siendo así que permite un acercamiento a la temática no tratada arduamente. Buscando poder dar una respuesta al problema formulado.

La finalidad de este trabajo es investigar si el revisor fiscal a través de su plan de trabajo fortalecer los sistemas de seguridad para disminuir la posibilidad de que organizaciones sean víctimas de delitos informáticos.

Definición del problema

En estas épocas el mundo no estaba preparado para lo que se avecinaba, nunca nadie podría haber sospechado lo que iba a deparar un año que suponía muchas expectativas para cada persona. El comienzo de la pandemia de Covid-19 ha generado diferentes consecuencias, desde el cierre de diferentes empresas hasta la muerte de personas

Una de esas consecuencias, son los delitos informáticos que en este último año han aumentado gradualmente (59% en comparación al año anterior), puesto que Colombia, ha cambiado alguna de sus actividades a modo virtual. Donde las empresas manejan la mayor parte de su información por este medio, por lo cual son propensas a ser víctimas de cibercrimen (Delitos informáticos), con consecuencias muy graves, como lo son daños patrimoniales y económicos y pérdida de información total o relevante.

En la realización de sus obligaciones, el revisor fiscal emplea la mayor parte de la información de las empresas en las cuales presta su servicio. Pero ¿El revisor fiscal tiene verdadero conocimiento sobre procedimientos y herramientas que puedan mitigar este tipo de riesgos?, si es así ¿las está aplicando correctamente?, o ¿está adquiriendo la competencia adecuada para evitar, en su trabajo, este tipo de riesgo?

Pregunta de investigación

¿Podría un Revisor Fiscal, bien capacitado, a través de su plan de trabajo gestionar para fortalecer los sistemas de seguridad para reducir la posibilidad que las organizaciones sean víctimas de delitos informáticos?

Objetivos

Objetivo General

Fortalecer el trabajo de los revisores fiscales para lograr disminuir la posibilidad de que las empresas sean víctimas de delitos informáticos.

Objetivos Específicos

Describir los antecedentes y consecuencias que ha generado la pandemia por COVID-19 a las organizaciones de Colombia.

Indagar cuales han sido los delitos informáticos contra las organizaciones más recurrentes durante los últimos cinco (5) años en país.

Indagar los programas académicos sobre ciberseguridad para que el revisor fortalezca su gestión a través de su plan de trabajo.

Marco teórico

Hace un tiempo, el mundo creía que las cosas no podrían estar peor, la vida no estaba tan bien, pero era la mejor posible, y se vivía bien dentro de lo que cabe. Sin embrago, un año atrás la pesadilla comenzó. La aparición de una enfermedad letal que se propagaba rápidamente, haciendo que el ser humano se confinara hasta tal grado que, los países en donde había más casos, las calles quedaran vacías.

"El Covid-19, es una enfermedad causada por el nuevo coronavirus de nombre científico SARS-CoV-2". (Organización Mundial de la Salud (OMS), 2020). Los coronavirus son un virus que causa Infección Respiratoria Aguda, que aparecen periódicamente en cualquier parte del mundo, es decir, que es una gripe que puede ser liviana, discreta o severa.

La Organización Mundial de la Salud (OMS), conoció por primera vez esta enfermedad cuando fue conocedora de un conjunto de casos de neumonía vírica el 31 de diciembre de 2019, declarado en Wuhan, República Popular de China. La neumonía vírica es una hinchazón o inflamación del tejido pulmonar causado por un microbio o virus.

En Wuhan, entre el 18 y 29 de diciembre de 2019, aparecieron los cinco primeros casos, donde cuatro pacientes fueron hospitalizados por presentar infección respiratoria aguda y uno de ellos falleció. De lo cual, la mayoría de ellos tenían conexión directa o indirecta con un mercado de despensas ubicado en Wuhan, provincia de Hubei.

Para el 1 de enero de 2020, el mercado cerró y no había evidencias claras del origen de esta enfermedad. El 2 de enero se reportaron 41 casos hospitalizados y el mismo número de muertes. El 7 de enero, China había descubierto una clase de coronavirus denominad 2019-nCoV.

El 12 de enero del 2020 se le dio por nombre Covid-19, suponiendo que este no era contagioso ya que no había registro de contagio de ser humano a ser humano, puesto que para

ese día no había nuevos reportes de casos relacionados y se asumió que se habían contagiado en el hospital o en el mercado cerrado que era el lugar de origen de esta enfermedad.

Unos 10 días después, 571 casos fueron dados a conocer en 25 diferentes provincias en China, mientras tanto, en Hubei, 17 casos registrados y 95 se mantenían en estado crítico. Desde ese momento los contagios crecían rápidamente en China continental, donde para el 30 de enero había 9.692 casos en China y 90 en países como Estados Unidos, India, Singapur, Taiwan, Vietnam, Tailandia, Malasia, Camboya, Alemania, Iran, Francia, y demás países.

El 19 de enero, llegó a un centro de salud un hombre que tenía 35 años presentando tos y fiebre, con antecedentes de visita familiar a Wuhan; fue el primer caso que surgió en el continente americano en el Estado de Washington, EE. UU. En enero 24, en Europa aparece el primer caso de esta enfermedad específicamente en Bordeaux, Francia, quien había visitado recientemente China.

Un hombre anciano de Sao Paulo, viajo recientemente a Lombardía, Italia, quien presento síntomas ligeros; quien fue el 1er caso reportado el 26 de febrero por el Ministerio de Salud de Brasil. El 6 de marzo del 2020 fue registrado en Colombia, el primer caso por Covid-19, quien era una paciente procedente de Milán, Italia.

Para el 11 de marzo había 4.291 personas fallecidas y 118.000 casos reportados y. Donde la OMS declara esta enfermedad como pandemia.

Acabado el año 2020, los casos y muerte seguían creciendo, sin embargo, ya no exponencialmente, habíamos vivido el primer pico de la pandemia. A continuación, se presentarán el total de los casos activos en Colombia desde el 31 de diciembre de 2020 hasta el 13 de marzo de 2021.

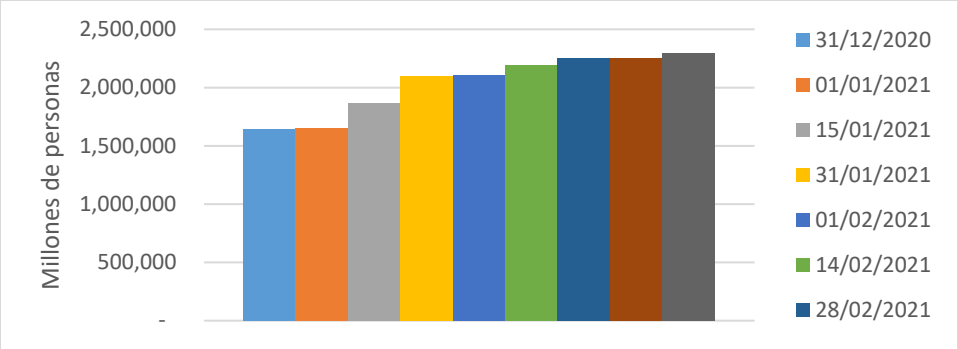

Figura 1. Total casos Covid-19

Nota: Fuente. Noticias. Elaboración propia

La anterior figura demuestra que como tal los casos no crecen exponencialmente si no que entre el día final del mes y al principio del otro hay un aumento de menos de 1%, equivalente entre las 10.000 y 13.000 personas.

Por otro lado, las consecuencias del Covid-19, a nivel salud son impactantes, puede dañar el corazón, el cerebro y los pulmones, haciendo aparecer los problemas de salud ya controlados o los que no se habían detectados. (El comercio, 2021), es decir, la persona contagiada puede quedar con secuelas. Segundo la muerte de muchas personas, desde familiares hasta desconocidas.

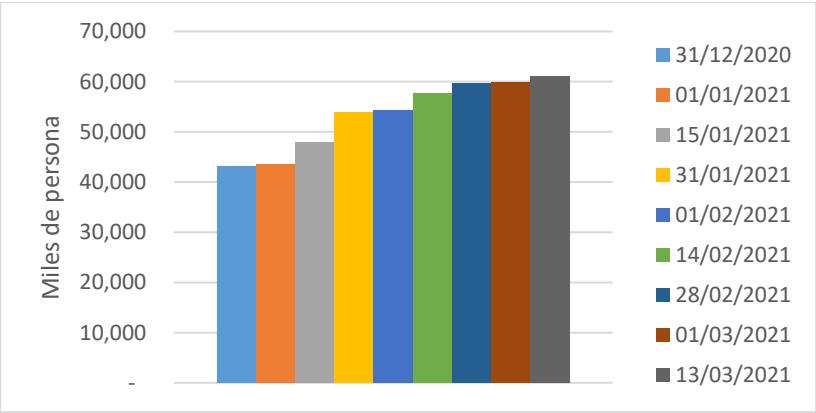

Figura 2. Total de muertes por Covid-19

Nota: Fuente. Noticias. Elaboración propia.

La anterior figura demuestra el total de muertes en Colombia donde entre el día final del mes y al principio del otro hay un aumento de menos de 1%, equivalente personas, equivalentes a no más de 100 personas al día.

Tabla 1.

Total, casos y muertes por Covid-19, 2020-2021

FECHA	TOTAL MUERTES	TOTAL CASOS
31/12/2020	43.213	1.642.775
01/01/2021	43.495	1.654.880
15/01/2021	47.868	1.870.179
31/01/2021	53.983	2.094.884
01/02/2021	54.272	2.104.506
14/02/2021	57.605	2.195.039
28/02/2021	59.766	2.251.690
01/03/2021	59.866	2.255.260
13/03/2021	61.046	2.299.082

Nota. Fuente: Noticias. Elaboración propia.

Se observa en la anterior tabla, el total de muertes y casos por Covid-19, como se observa cada parte crece continuamente, por una parte, los aumentos son bajos en otras son altos.

Existen varias consecuencias, sin embargo, se hablará sobre los delitos informáticos específicamente la ciberseguridad. Los delitos informáticos es toda aquella acción, típica, antijurídica y culpable, dada por vías informáticas cuyo objetivo es destruir y dañar ordenadores, medios electrónicos y redes de Internet. (Buitrago, 2015). Es toda acción antijurídica que se realiza a través de un espacio digital, internet o entorno digital.

Este tipo de delitos es difícil de demostrar, ya que, en su mayoría, las evidencias no son encontradas o pero aún son difíciles de buscar. Es así que estos actos se realizan de manera rápida durando solo unos segundos y sin que la víctima se dé cuenta, no necesariamente debes estar físicamente y únicamente se necesita la utilización de un dispositivo informático.

Igualmente, el pasar de los años, los delitos informáticos evolucionan y aumentan, siendo más difícil la identificación y persecución de los mismo.

Con la evolución de la tecnología y las circunstancias en las que Colombia se encuentra, los delitos informáticos se hacen cada vez más y más habituales. Y en esta categoría de delitos, existen diferentes clases de crímenes, de los cuales están definidos en la ley 1273 de 2009

Estas clases de crímenes son: acceso ilegal a un sistema informático (Art. 269A), no tener autorización y accede en parte o completamente a un sistema informático; obstaculización ilegitima de sistemas informáticos o redes de telecomunicaciones (Art. 269B), sin autorización alguna impida el ingreso o funcionamiento a datos informáticos, a sistemas o a redes de telecomunicaciones; apropiación de datos informáticos (Art.269C), sin previa orden judicial obstruya los datos desde su destino, su origen o en el interior de un sistema; daño informático (Art. 269D), el que suprima, borre, deteriore, destruya o altere datos o sistemas informáticos; usos de software malicioso (Art. 269E), el sin estar autorizado introduzca, extraiga, produzca, distribuya, venda, trafique, adquiera o venda del territorio nacional; violación de datos personales (Art. 269F), sin estar autorizado, para beneficio propio o de terceros compile, ofrezca, sustraiga, intercepte, venda, obtenga, modifique, emplee, compre, intercambie, envíe o divulgue del territorio nacional datos personales en medios informáticos; y reemplazo de sitios web para apoderarse de datos personales (Art. 269G), sin autorización alguna y con objetivo ilícito desarrolle, diseñe, programe, ejecute, venda, envíe o trafique enlaces, ventanas emergentes o páginas electrónicas.

Así mismo, para las empresas que hoy en día han necesitado un cambio de operación como lo son el tratamiento de cualquier tipo de información, ha generado beneficios como mejor organización en cuanto a sus datos; también ha traído consigo riesgos inherentes llamados

riesgos cibernéticos o informáticos como lo son: fraude informáticos, robo o manipulación de información privada o confidencial, e implementación de software malicioso que tiene como consecuencia el daño de hardware, destrucción de datos, interrupción de la operación de la entidad e incapacitación de los sistemas de esta.

Es así como, en este documento, se quiere comprender como podría el Revisor Fiscal reducir los delitos informáticos a tal manera de que las organizaciones no pierdan dinero como también ninguna clase de pérdidas. Para ello definiremos primero la revisoría fiscal y después el revisor fiscal.

La Revisoría Fiscal le compete dictaminar los EEFF (estados financieros), que es un órgano de fiscalización, que también le incumbe evaluar y revisar constantemente los elementos y componentes que constituyen el control interno, en forma independiente, oportuna y objetiva.

Este órgano lo ejerce un Revisor Fiscal, que es un auditor que a su vez es un Contador Público, donde su nombramiento legal y jurisdicciones están plasmadas parcial o totalmente en la Ley 145 de 1960, en la Ley 43 de 1990, en el Estatuto Tributario y en el Código de Comercio.

El Revisor Fiscal tiene diferentes funciones que están escritas en el artículo 207 del Código de Comercio, hay se aprecia que no solamente es dictaminar los estados financieros de una compañía, sino que va más allá de ello hasta llegar a donde le sea posible al ejercer sus obligaciones. Sin embargo, algunos simplemente van a dictaminarlos, es decir, ponen su firma para hacer más rápido su trabajo. Es así que “La labor realizada por el revisor fiscal en las organizaciones, en la mayoría de las ocasiones responde más al cumplimiento de una obligación legal que a la comprensión de la necesidad del control para asegurar el logro de los objetivos en las mismas”. (Jaramillo, 2014).

Ir más allá no significa salirse de lo que es el cumplimiento de las funciones, es agregar valor a lo que se ejecuta, es dar confianza a los inversionistas, al Estado y a la sociedad. Por ello la mayoría de las empresas aplican herramientas como la ciberseguridad para reducir el riesgo cibernético, es "el uso de los mecanismos tecnológicos como programas informáticos, sistemas de hardware que evitan que los intrusos informáticos tengan acceso a las bases de datos de las organizaciones con fines de lucro". (Cruz, 2018).

La seguridad de la tecnología de la información, es el modo de defender los datos informáticos, dispositivos móviles, las redes, los sistemas informáticos, los servidores y las computaras ante el ataque de personas externas o de la misma información con beneficio propio o de terceros.

La empresa debe aplicar la ciberseguridad puesto que en estos tiempos de pandemia está más propensa a los diferentes delitos informáticos ya mencionados. Esta tiene que estar incursionada primeramente en el Gobierno Corporativo, a su vez se debe crear las tres líneas de defensa para la gestión de riesgos.

La primera línea de defensa está posicionada en la operación, trata sobre la caracterización, evaluación, control y mitigación de riesgos, para guiar el desarrollo e implementación de procedimientos y políticas internas, con el fin de realizar un mantenimiento efectivo a los controles internos y procedimiento de medición del riesgo operativo.

La segunda línea de defensa, en esta se debe definir las normas claras, los procedimiento y directrices para el marco de control de cada riesgo, establecidos en una política o manual. Esta da apoyo y asesoramiento a la primera línea de defensa evaluando su eficacia y garantizando que cada riesgo este definido en un marco de control.

Por último, la tercera línea de defensa está a cargo de los auditores internos, donde deben ser independientes de las dos líneas anteriores, lo cual concede un nivel alto de garantía la gestión de riesgos, controles internos, la eficacia del gobierno y la manera en que la primera y segunda línea cumplen sus objetivos de gestión de riesgos y control.

En todo esto entra el revisor fiscal puesto que…

> Las funciones del revisor fiscal van más allá del dictamen de los estados financieros: es una figura esencial cuya vigilancia del buen hacer y apego a las normas en comunidad son garantía de confianza para inversionistas, el Estado y la sociedad en general sobre el actuar de empresas y sus administradores. (Bermudez, 2011).

También vigila el sistema de control interno, sus objetivos como su cumplimiento que estén acorde a los objetivos de la organización, cada uno de sus componentes. Estas líneas anteriores deben estar implementadas en el sistema de control interno para lograr una efectiva gestión del riesgo con la participación del Revisor Fiscal.

No únicamente el Revisor Fiscal se debe enfocar en las tres líneas de defensas anteriores, puesto que así mismo que se implique no garantiza la protección de la información que maneja. Por eso este se debe ir más allá, seguir adquiriendo conocimientos a través de diferentes capacitaciones sobre la ciberseguridad, como lo pueden ser maestrías y especializaciones.

Depende de cada uno de los revisores fiscales el crecer en su profesión y garantizar la información proporcionada por la entidad y el de su trabajo sea verdadera para la ciudadanía. No quedarse estancado en únicamente dictaminar los estados financieros, sino que también el garantizar que las actividades del sistema de control interno estén realizadas de acuerdo a lo establecido en la entidad.

Conceptos básicos

Riesgo cibernético

Cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información. (Banco de la República, 2016).

Delitos informáticos

Son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc. (Policia Nacional de Colombia, s.f.).

Ciberseguridad

Es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. (Infosecurity, s.f.).

CRI

Índice de ciber riesgo

Criptografía

Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. (Venturi, 2020).

OWASP

Proyecto abierto de seguridad de aplicaciones web

Ethical Hacking

Se define a través de lo que hacen los profesionales que se dedican a ello, es decir, los piratas informáticos éticos. Estas personas son contratadas para hackear un sistema e identificar y reparar posibles vulnerabilidades, lo que previene eficazmente la explotación por hackers maliciosos. (Cámara Valencia, s.f.).

Compliance

Cumplimiento normativo, normas establecidas por las empresas en los ámbitos interno y externo. (Melchior & Ducom, s.f.).

Ciber resiliencia

Capacidad de una empresa de adaptarse y continuar con sus funciones y su trabajo en situaciones de riesgo. (Tecon, s.f.).

Pentesting

También llamado “test de penetración” consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos. (Prenafeta, 2018).

Repercusiones de la pandemia del COVID-19

La pandemia por COVID-19 ha dejado atrás consecuencias graves para la humanidad, como lo es la muerte de cientos y cientos de personas a lo largo del mundo. Colombia, como muchos otros países, ha sufrido varias consecuencias en diferentes sectores como lo son la salud, la economía, la sociedad y a nivel de entidades.

En el sector salud, los resultados son cierres de los institutos prestadores de salud (IPS), cierre de las unidades de servicios dentro de las instituciones hospitalarias como las UCI (unidad de cuidados intensivos), por la causa del aumento de contagiados como el personal de salud de estos. Lo cual puede generar la disminución de camas disponibles de UCI en el país.

También, a nivel de los diferentes sectores ya mencionados, se observa un aumento de los despidos a trabajadores, como en el sector salud, por la pandemia, recortando sus nóminas o simplemente disminuyen un porcentaje, a las veces significativos, en el pago de los honorarios de los médicos.

A nivel económico, el impacto ha sido el más fuerte, para el 2019 Colombia había tenido un buen desempeño que alcanzó una tasa de crecimiento del 3,3%. Sin embargo, estimaban que, en 2020, obtuviera un crecimiento económico cerca del 3,5%. Pero, las cosas fueron diferentes, en el primer trimestre de ese año. Colombia sufrió dos circunstancias que suponen graves resultados para la economía mundial a corto y largo plazo, como lo son la pandemia por Covid-19 y la caída internacional del precio del petróleo.

Por otro lado, la sociedad está enfrentando situaciones como la muerte de familia, conocidos y desconocidos. Así mismo, hay una mayor preocupación en Colombia, el aumento del desempleo en comparación de un año a otro es grande, puesto que los trabajadores han sido relevados de su cargo. A continuación, se presenta la tasa de desempleo entre 2015 – 2020:

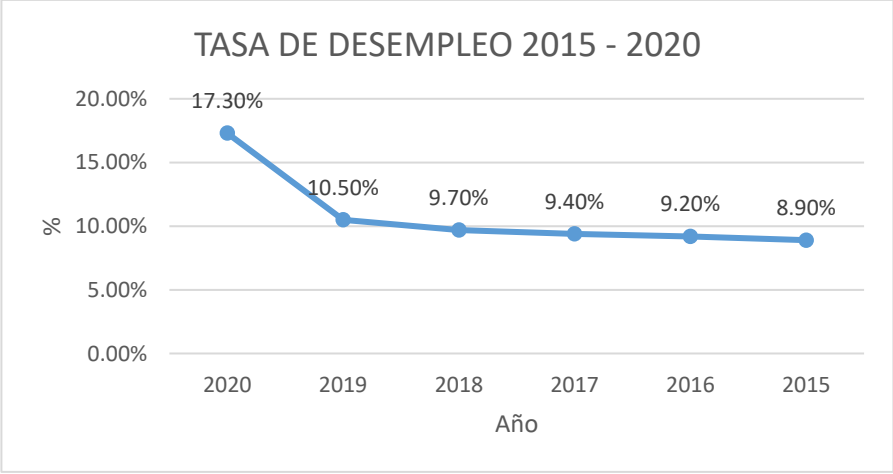

Figura 3. Tasa de desempleo (%)

Nota: Fuente: Knoema. Elaboración propia

Como se observa entre los años 2019 y 2020 hubo un crecimiento del casi 7%, finalizando con una tasa de desempleo mayor al 17%, implicando que la pandemia dio como resultado el incremento de del desempleo. Esta situación es la principal consecuencia de la pandemia.

A nivel empresarial, las consecuencias han sido fatídicas, miles de empresas pequeñas y micro han tenido que cerrar por falta de liquidez, algunas pudieron mantenerse por dos meses más con recursos propios, puesto que no podían solventar un préstamo, pero posteriormente finalizaron sus operaciones.

Además, hay algunas medidas que, durante la pandemia en el 2020, adoptaron las empresas y una de ellas les costaría pérdidas económicas mayores de las que han tenido en años anteriores en cuanto a ese ítem, que son las ventas o prestaciones que disminuyeron debido al cese de actividades. Lo cual lo utilizaron el 37% de las empresas encuestadas. A continuación, las medidas adoptadas:

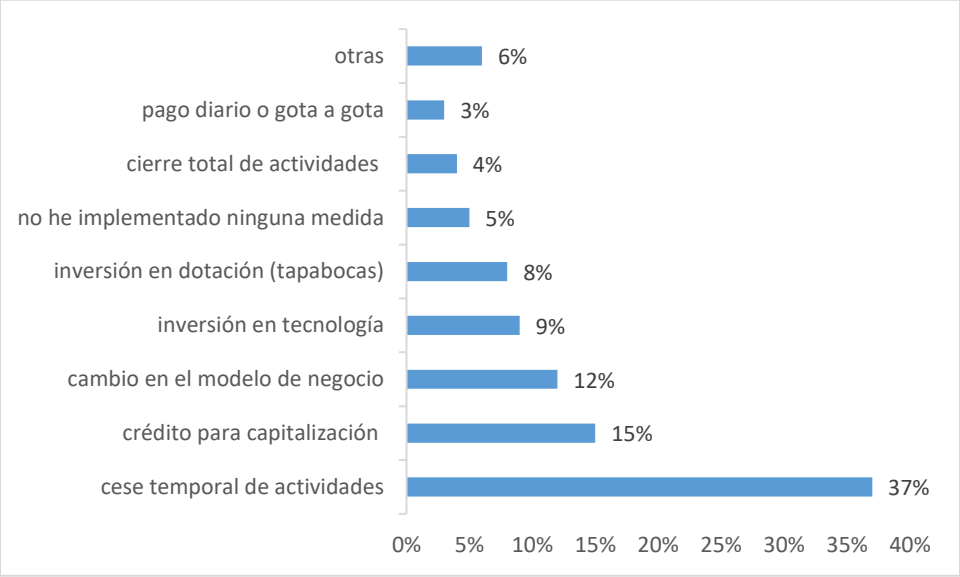

Figura 4. Medidas adoptadas por las empresas debido al Covid-19

Nota. Fuente: Cámara de Comercio de Bogotá. Elaborado por. (Cámara de Comercio de Bogotá, 2020).

Debido a las medidas acogidas por el gobierno nacional por contener la pandemia de coronavirus, además de las aplicadas por las empresas, el 96% reportaron que sus ventas habían disminuido y el 4% que se mantenían iguales.

Además, las empresas no poseen tanta capacidad financiera para cumplir sus obligaciones, como arrendamientos, deudas, servicios públicos, y demás; el 50,1% las puede consumar en menos de 1 mes, el 43,4% entre 1 a 3 meses y el 6,5% en más de 3 meses. En donde 1 de cada 10 empresas tiene la capacidad de cumplirlas en más de 3 meses.

Esta fue una encuesta aplicada a 631 empresas, en donde la mayoría son microempresas entre el 1 y 20 de abril del año 2020. Según esta encuesta los más afectados son las pequeñas (17%) y microempresas (72%) de los sectores de servicios (45%), comercio (27%) e industria (22%).

También a nivel de empresas, los delitos informáticos han crecido exponencialmente, también llamados Cibercrimen, los cuales hacen perder millones de millones de dinero a las entidades. Según el reporte del Centro Cibernético de la Policía Nacional, estos se incrementaron en un 59% en los primeros 6 meses del 2020. Es así como entre enero y junio de 2020 denunciaron 17.211 denuncias, más de 6.340 en comparación al primer semestre del 2019. Además de que los casos de suplantación de sitios web, aumentó exponencial, el 364% respectivo a 2.103 casos.

Delitos informáticos en Colombia

Los delitos informáticos o cibercrimen han aumentado radicalmente en el año 2020 a lo largo de la evolución de la pandemia. El cambio de la mayoría de las actividades de los

colombianos y las empresas los ha vuelto más propensos a este tipo de fraude. Su crecimiento se muestra a continuación:

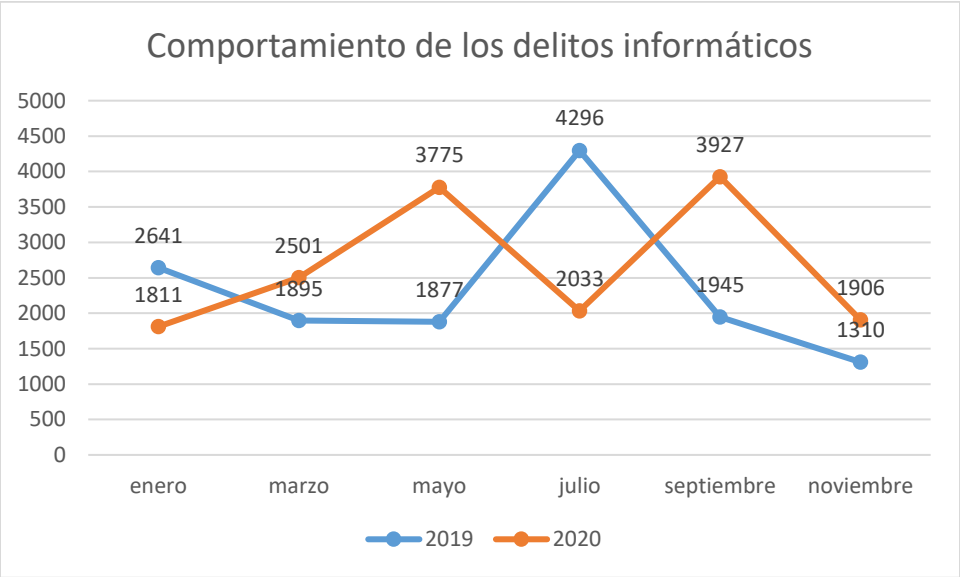

Figura 5. Comportamiento de los delitos informáticos 2019-2020

Nota. Fuente: Asuntos: Legales. Elaboración propia

A corte de noviembre del 2020 se observó un incremento del 83% de los delitos realizados por medios informáticos, puesto que de 21.107 paso a ser 36.834 de delitos en 2020. Estas cifras son dadas en general sin embargo no se posee certeza de que sean verdad, aunque fueron investigadas de diferentes fuentes de información.

Así mismo, aumentaron exponencialmente los diferentes tipos de delitos informáticos en Colombia, comparado con el año 2019 y el año 2020. Estos se exponen en la siguiente tabla:

Tabla 2.

Delitos informáticos que crecieron en 2020

Modalidad	Cantidad Año 2019	Cantidad Año 2020	Variación Porcentual
Correo electrónico, spam y scam	4	41	935%
Suplantación de sitios web	892	4776	435%
Modificación de datos o registros personales	136	677	398%
Extracción de datos o registros personales	563	2663	373%
Suplantación de identidad por correo ajenos	333	1527	359%
Introducir o extraer del país software maliciosos	4	17	325%
Simulación de app move (fake app)	58	238	310%
Suplantación blog	2	8	300%
Ingeniería social	107	427	299%
Capturas de tramas de red de computadores (sinffer)	15	56	273%

Nota. Fuente: Asuntos: legales. Elaborado por (Argote, 2021).

Se observa en la anterior tabla, que el mayor crecimiento según cantidad para el año 2020 fue el de suplantación de sitios web con 4.776 casos y una variación porcentual de 435%, este tipo de delito es el más común puesto que para los cibercriminales, el avance de la tecnología y el desconocimiento de las empresas, los profesionales y la ciudadanía sobre ello es un punto a favor que saben aprovechar.

Por otro lado, si se habla sobre la mayor variación porcentual la tiene la modalidad de correo electrónico, spam (Correo electrónico no deseado) y scam (Estafas por medios electrónicos) con

925%, que paso de 4 a 41 casos de 2019 a 2020 correspondientemente. En la menor cantidad se encuentra la suplantación del blog con 8 casos en 2020 y una variación porcentual del 300%, sin embargo, se encuentra la modalidad de capturas de tramas de red de computadores (Sinffer) en la menor variación porcentual con 273% y 56 casos reportados en el año 2020.

Al igual que aumento esos delitos también hubo otros que tuvieron una disminución radical.

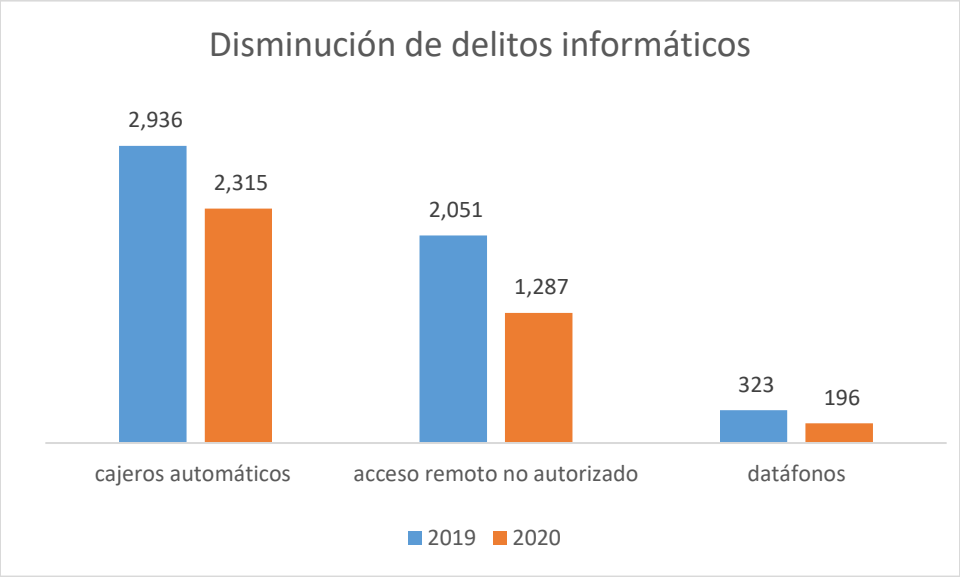

Figura 6. Disminución de los delitos informáticos

Nota. Fuente: Asuntos legales. Elaboración propia

Como se evidencia únicamente estas tres modalidades sufrieron una caída. Los cajeros automáticos presentaron una disminución del 21% con una variación de – 621 casos reportados en comparación de 2020 a 2019. Así mismo, el acceso remoto no autorizado obtuvo una variación porcentual del – 37% disminuyendo en 764, siendo esta modalidad la mayor en decrecimiento según cantidad de casos reportados. Por otro lado, esta los datafonos los cuales tuvieron una mayor variación porcentual, – 39%, pasando de 323 a 196 casos.

Además, cerca del 90% de los ciberataques o delitos informáticos contra las organizaciones en Colombia es debido a la ingeniería social, esta "implica manipulación para obtener información confidencial, como datos personales o financieros" (Bodnar, 2021). Es decir, que los criminales manipulan a los usuarios legítimos de una empresa con el fin de conseguir ingreso, permisos o información de sistemas de información para hacer daño a la entidad o persona.

De allí sale los ataques BEC (Business Email Compromise), consiste en suplantar por medio de correos corporativos a los gerentes generales o financieros con el de que puedan transferir sumas de dinero a cuentas bancaria y tener acceso a las finanzas de la entidad. También consiguen suplantar a sus proveedores y clientes por medio del robo de identidades apoyado en ingeniería social.

También, los cibercriminales utilizaron más las modalidades de suplantación de identidad por medio de correos maliciosos (Phishing) para estafar a los CEO, apoderándose de su correo corporativo generando comunicados falsos a los empleados relacionados directamente de realizar transferencias y dispersar pagos.

En Colombia, el Ransomware "programa de software malicioso que infecta computadoras y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema". (Kaspersky, s.f.), además es una ciberamenaza que es subestimada puesto que no es vista a menudo, pero, igualmente es un ataque que los criminales a través del uso de criptomonedas monetizan sus ganancias. Un Ransonware es un software malicioso que puede bloquear totalmente un equipo de computador a través del envío de un correo que contiene archivos infectados que los usuarios finales descargan y así bloquean y pueden obtener información relevante o total.

El ataque DDOS (Ataque de denegación de servicio), tiene la finalidad de inhabilitar el uso de una aplicación, un servidor o sistema para bloquear un servicio destinado. Según el Centro Cibernético Policial, 170 empresas reportaron este tipo de ataque que lograron interrumpir sus servicios de frente a sus clientes, causando daños graves operativos y reputacionales.

Programas académicos de ciberseguridad

Un mecanismo o herramienta que se ha utilizado a lo largo del tiempo, pero que no ha tenido gran reconocimiento en estos últimos años, que tiene la finalidad de reducir los riesgos sobre la información manejada y almacenada es la Ciberseguridad. No muchos tienen conocimiento sobre ella, o no saben o realmente no la manejan, pero si la conocen.

Aunque durante el 2020 hubo inversión en seguridad que alcanzo $10.400 millones por el Covid-19, Colombia ocupo el puesto 39 en el raking mundial de ciberseguridad, el 60% de los fraudes se origina en dispositivos móviles, más de 24.000 aplicaciones móviles maliciosas se bloquean cada día. Se evidencia que esta herramienta no es utilizada de la manera correcta, puesto que, aunque solamente tengan conocimiento los profesionales relacionados con la informática o la tecnología, esta situación no abarca totalmente todas las áreas o departamentos de las organizaciones respectivamente.

Es así como, aunque el control interno tome medidas respecto a estos riesgos, la falta de conocimientos en la mayoría del personal o persona contratada por la entidad genera que la empresa este vulnerable ante los cibercriminales, puesto que específicamente el Revisor Fiscal tiene la función de avalar que las actividades del sistema de control interno se cumplan correctamente y sean acordes con la organización.

El Revisor Fiscal puede capacitarse en lo que respecta a la ciberseguridad para que pueda proteger la información que maneja a lo largo de su trabajo. Es así como se investigó sobre

capacitaciones de diferentes estudios como los son maestrías, diplomados, especializaciones y demás que puedan ayudar al revisor fiscal a obtener conocimientos con el fin de evitar estos delitos informáticos.

Tabla 3.

Investigación estudios en ciberseguridad

DIPLOMADOS	
Diplomado en Ciberseguridad	
Universidad	Universidad Manuela Beltran
Duración	120 horas
Inversión	$1.498.000
Modalidad	Virtual
Descripción	Muestra la forma de aprovechar la ciberseguridad y sus aplicaciones, utilizando herramientas tecnológicas
Plan de estudios	**Módulo 1:** Seguridad en sistemas operativos Tema 1: Seguridad en sistemas operativos: ofrece un marco conceptual, definiciones de seguridad informática y mecanismos de seguridad de cada sistema operativo Tema 2: Seguridad en el software: ofrece aspectos generales de esta seguridad, metodologías de desarrollo de software seguro y el TOP 10 de OWASP (proyecto abierto de seguridad de aplicaciones web) Tema 3: Criptografía: ofrece marco teórico, de este salen conceptos generales, criptografía simétrica, asimétrica y algoritmos de reducción o resumen de mensajes **Módulo 2**: Ethical Hacking Tema 1: Conceptos generales Ethical Hacking: generalidades, amenazas de seguridad, tipos de ataques y vectores de ataque Tema 2: Tipos de Ethical Hacking: Hacking de sistemas, de redes y de servidores Tema 3: Procesos de seguridad Ethical Hacing: pruebas de penetración y herramientas del Ethical Hacking **Módulo 3:** Seguridad informática Tema 1: Ingenieria social: conceptos generales, principios básics, tipos de ataques y ¿Cómo protegerse de la ingeniería social? Unidad Tema 2: Analisis forense digital: introducción, fases y herramientas Tema 3: Gestión de seguridad informática: aspectos generales, SGSI (ISO 27001), análisis de riesgos de seguridad informática (ISO 31000) y metodologías para el análisis de riesgos.
Link	https://umb.edu.co/programa/diplomado-en-ciberseguridad/
Diplomado Ciberseguridad y Compliance	
Universidad EAN	

	90 horas $3.010.000 Ofrece conocimientos y herramientas para aportar en la planeación, gestión y disposición de controles efectivos en materia de ciberseguridad y cumplimiento en las organizaciones. Módulo 1: Riesgos, aborda las temáticas asociadas con riesgos cibernéticos, la normatividad y el compliance (cumplimiento normativo, normas establecidas por las empresas en los ámbitos interno y externo), el impacto organizacional y buen gobierno en materia de cumplimiento. Duración 24 horas Módulo 2: Legislación: aborda las tipologías y modalidades asociadas al cibercrimen, y la legislación aplicable en materia de compliance. Duración 42 horas Módulo 3: Ciberseguridad: aborda acerca de los estándares asociads a la ciberseguridad y la noción de ciber resiliencia (capacidad de una empresa de adaptarse y continuar con sus funciones y su trabajo en situaciones de riesgo). Duración 24 horas https://universidadean.edu.co/programas/diplomados/diplomado-ciberseguridad-y-compliance

ESPECIALIZACIÓN	
4	**Especialización Ciberseguridad Organizacional**
Universidad	Universidad Autónoma de Bucaramanga
Duración	2 semestres
Inversión	Tota: $13.900.000; Semestral: $6.952.000
Modalidad	Presencial
Créditos	22
Descripción	Ofrece conocimientos en ciberseguridad, seguridad de la información, cibercrimen, ciberterrorismo, confidencialidad de datos y buenas prácticas en ciberseguridad organizacional que les permite participar en los objetivos estratégicos de la organización.
Plan de estudios	Primer semestre - Electiva I - Fundamentos en ciberseguridad - Liderazgo para el cambio - Seminario I - Solución creativa de problemas - Tecnologías de información Segundo semestre - Amenazas informáticas - Electiva II - Gestión de seguridad de la información - Marco regulatorio en ciberseguridad - Seminario II - Tendencias en ciberseguridad
Link	https://www.unab.edu.co/programas/ciberseguridad-organizacional-especializaci%C3%B3n-presencial-bogot%C3%A1

ESPECIALIZACIÓN	
5	**Especialización en seguridad de la información con énfasis en consultoría**
Universidad	Politécnico Gran Colombiano – Institución Universitaria
Duración	2 cuatrimestres
Créditos	60

Descripción	Existe doble titulación, donde los egresados del programa de la especialización en seguridad de la información tienen la posibilidad de realizar una doble titulación en estudios de maestrías oficiales en un año con titulación europea online y reconocimiento de créditos automáticos.
Plan de estudios	Primer cuatrimestre - Aspectos legales y regulatorios - Gestión de la seguridad - Seguridad en redes - Seguridad en sistemas operativos - Análisis forense - Criptografía y mecanismos de seguridad - Análisis de vulnerabilidades Segundo cuatrimestre - Análisis de riesgos legales - Auditoría de la seguridad - Seguridad en aplicaciones online y bases de datos - Seguridad en el software - Delitos informáticos - Trabajo fin máster
Link	https://www.poli.edu.co/dobletitulacion/especializacion-en-seguridad-de-la-informacion

MÁSTER	
6	**Máster Universitario de ciberseguridad y privacidad**
Universidad	Universidad Oberta de Catalunya
Duración	2 semestres
Modalidad	Virtual
Créditos	60
Descripción	El máster ofrece la posibilidad de intensificar el perfil profesional del estudiante cursando una de las tres especialidades siguientes: **Sistemas (18 ECTS):** Enfocada a entender los mecanismos de prevención, protección y detección de vulnerabilidades, y adquirir las competencias del hacking ético y del pentesting. También se focaliza en la identificación de ataques y en la recogida de evidencias digitales a través de las metodologías de la informática forense. **Tecnologías (18 ECTS):** Se centra en conocer herramientas que permitan crear servicios y aplicaciones con las máximas garantías de seguridad y privacidad: desde protocolos de bajo nivel para el control de acceso (por ejemplo RADIUS), a tecnologías DLT (Distributed Ledger Technologies) y en especial al sistema de Blockchain (incluyendo bitcoins y ether) para desplegar sistemas distribuidos que garanticen la integridad de los datos, pasando por metodologías y herramientas de software seguro e ingeniería inversa. **Gestión (18 ECTS):** Gestión de la seguridad, en concreto en conocer como desplegar sistemas de gestión de la seguridad según la normativa ISO 27001, al hacer auditorías técnicas de certificación, o al tener competencias para gestionar los activos empresariales en la nube de forma segura.
Plan de estudios	Asignaturas obligatorias: - Legislación y protección de datos - Fundamentos de ciberseguridad - Privacidad Especialidad 1: Sistemas - Seguridad y pentesting de servidores de datos - Seguridad y pentesting de sistemas - Análisis forense Especialidad 2: Tecnologías - Seguridad del software - Sistemas de blockchain - Arquitecturas y protocolos de seguridad Especialidad 3: Gestión

	- Sistemas de gestión de la seguridad - Seguridad en cloud computing - Auditoría técnica Optativas - Dirección estratégica de sistemas y tecnologías de la información - Técnicas de investigación - Modelos avanzados de minería de datos - Ciberdelitos: estudio de los tipos delictivos - Criptografía avanzada - Biometría - Técnicas de ocultación de la información
Link	https://estudios.uoc.edu/es/masters-universitarios/ciberseguridad-privacidad/objetivos-perfiles-competencias

	MÁSTER
7	**Máster en Ciberseguridad**
Universidad	OBS Business School
Duración	12 meses
Inversión	7.500 euros
Modalidad	Online
Créditos	60
Descripción	Facilita a profesionales y directivos la definición de estrategias y el conocimiento de herramientas que permiten trabajar en torno a la seguridad de los datos, enfocados a garantizar la continuidad en las operaciones y la permanencia en los mercados. Te capacita para la dirección y gestión de los sistemas de seguridad de la información de las empresas, de tal manera que seas capaz de interactuar con consultores y expertos en seguridad informática, con el fin de promover e implementar estrategias capaces de blindar el conocimiento de las empresas
Plan de estudios	**Bloque 1:** Iniciación Tema 1: introducción a la seguridad de la información Tema 2: gobierno TI **Bloque 2:** Profundización Tema 1: gestión de la seguridad en arquitectura TI Tema 2: criptografía, sistemas de encriptación y protección Tema 3: seguridad en infraestructuras de comunicación Tema 4: gestión de proyectos TI Tema 5: fundamentos de cyberattack **Bloque 3:** Visión general Tema 1: marco legal y regulatorio Tema 2: evaluación y selección de sistemas de seguridad Tema 3: auditoría de sistemas Trabajo fin de máster **Actividades adicionales** - Taller: certificación CISM (certified information security management - Caso estudio: método del caso - Webinars
Link	https://www.obsbusiness.school/masters-online/master-en-ciberseguridad

	MAESTRÍA
8	**Maestría en ciberseguridad y ciberdefensa**
Universidad	Universidad Escuela Superior de Guerra (ESDEG)

Duración	3 semestre
Inversión	Valor inscripción: $151.200, valor matricula: $8.425.100
Modalidad	Presencial
Créditos	42
Descripción	Programa que integre conceptos, prácticas, y procedimientos propios de la seguridad de la información, las telecomunicaciones y el riesgo operacional; capaz de formular políticas, diseñar estrategias, tomar decisiones y gestionar conocimiento propio, para garantizar el cumplimiento de la misión de una organización y su resiliencia.
Plan de estudios	Semestre I - Contexto en ciberseguridad y ciberdefensa - Seguridad y defensa en el ciberespacio - Sistemas cibernéticos - Diseños de Investigación - Concepto operacional Semestre II - Regulaciones en ciberseguridad y ciberdefensa - Proyecto de investigación - Prospectiva en ciberseguridad y ciberdefensa - Administración de recursos cibernéticos - Electiva I Semestre II - Ética en el ciberespacio - Trabajo de investigación - Innovación en ciberseguridad y ciberdefensa - Electiva II
Link	https://esdegue.edu.co/es/maestria-en-ciberseguridad-y-ciberdefensa

CURSO	
9	**Curso virtual sistemas de gestión y auditoría para la seguridad informática**
Universidad	Corporación Universitaria UNITEC
Duración	8 semanas – 36 horas
Inversión	$815.000
Modalidad	Virtual Asistida
Créditos	3
Descripción	Preparar a los estudiantes y/o profesionales en el conocimiento de estrategias y herramientas enfocadas al análisis en el marco de la seguridad de la información.
Plan de estudios	Semana 1: Introducción a la seguridad informática. Semana 2: Fundamentos básicos de la ciberseguridad. Semana 3 Y 4: Introducción al análisis de vulnerabilidades. Semana 5: Metodologías de análisis de vulnerabilidades. Semana 6 Y 7: Herramientas de detección de vulnerabilidades. Semana 8: Aplicación de controles de vulnerabilidades.
Link	https://www.unitec.edu.co/programas/1716/curso-virtual-sistemas-de-gestion-y-auditoria-para-la-seguridad-informatica

PROGRAMA	
10	**Programa de protección cibernética para empresas**
Proporciona	Cámara de Comercio de Bogotá (CCB)
Inversión	Gratis
Modalidad	Virtual

Descripción	La CCB creo un programa gratuito e ilimitado en donde las pequeñas y medianas entidades de Bogotá y la Región pueden protegerse contra los delitos informáticos a través de la Iniciativa Cluster de Software y TI, y el Instituto de Preparación Cibernética (CRI). Incluye orientación en línea a través de cinco etapas: • Uso de USB y extraíbles • Autenticación de contraseña • Parcheo y actualización de software • Prevención de ataques de Phishing • Seguridad en la nube Dispone de la asesoría de expertos en ciberseguridad, del CRI Al obtener la herramienta, las empresas accederán a los recursos desarrollados por el CRI con la finalidad de dar apoyo a crear una cultura de preparación cibernética para su lugar de trabajo. Quienes se inscriban y tomen el programa podrán realizarlo a su propio ritmo, manejando tiempo y curva de aprendizaje. Una vez lo finalicen, podrán recibir un certificado de cumplimiento que otorga el CRI
Link	https://bogota.gov.co/mi-ciudad/desarrollo-economico/programa-gratuito-de-proteccion-cibernetica-para-empresas-bogotanas

Nota. Fuente: Universidades. Elaboración propia

El Diplomado en ciberseguridad de la Universidad Manuela Beltrán y el Diplomado en ciberseguridad y compliance de la Universidad EAN son muy diferentes en cuanto a su plan de estudios. El primero aborda temas de seguridad en sistemas operativos y en software, criptografía, la Ethical Hacking, sus tipos y procesos de seguridad, y por último seguridad informática que es la finalidad del programa académico con la utilización de normas ISO, está más enfocado al contexto.

El segundo diplomado, que el de la Universidad EAN aborda temas de aplicación, como los riesgos cibernéticos, normatividad de esos riesgos y de ciberseguridad y el compliance, además de impacto organizacional y buen gobierno en cuanto al cumplimiento. Después le sigue tipos y modalidades asociadas al cibercrimen, legislación de compliance, y por último está la ciberseguridad. Aquí abarca la ciberseguridad en cuanto a estándares y la noción de ciber resiliencia.

La especialización en seguridad de la información y la especialización en seguridad de la información con énfasis en consultoría del Politécnico Gran Colombiano y la especialización Ciberseguridad Organizacional de la Universidad Autónoma de Bucaramanga poseen casi el

mismo plan de estudios, pero lo expresan de diferentes maneras. No hay certeza de cuanto equivale la matrícula de cada una ellas, la diferencia más notable entre ellas es la doble titulación que se obtiene en la Especialización en Seguridad de la Información con énfasis en consultoría (titulación europea), pero abarca específicamente los delitos informáticos. La otra de la Universidad Autónoma de Bucaramanga, está enfocada a la práctica, es decir, amenazas, riesgos, solución a los problemas que es importante en la ciberseguridad; abarcando gestión, tendencias, marco regulatorio, tecnologías de la información y una que no lo plantea los otros estudios es: el liderazgo para el cambio.

El Máster Universitario de Ciberseguridad y Privacidad de la Universidad Oberta de Catalunya, aunque va dirigido a los ingenieros y a fines, brinda la posibilidad de enfocarse en cualquiera de las tres especialidades: sistemas, tecnologías o gestión, ¿Cuál de ellas es mejor? No se sabe, cada una abarca diferentes temas, también esta ofrece técnicas de investigación, estudio de tipos delictivos (ciberdelitos), biometría y técnicas de ocultación de la información.

El Máster en Ciberseguridad del OBS Business School abarca seguridad de la información, en las TIC, en infraestructuras de comunicación, además ciberataque, sistemas de seguridad y auditoría de sistemas, también ofrece casos estudios, certificaciones y webinarios, lo que no lo hacen las otras.

La Maestría en Ciberseguridad y ciberdefensa de la Universidad ESDEG abarca la ciberseguridad, la ciberdefensa, cibernética y ciberespacio; además de diseño, proyecto y trabajo de investigación y la ética en el ciberespacio.

El curso virtual llamado Sistemas de Gestión y Auditoría para la Seguridad Informática de la Corporación Universitaria UNITEC brinda seguridad informática, fundamentos de la

ciberseguridad y vulnerabilidades, dura muy poco, pero aborda algunos temas a los anteriores estudios.

Y el programa de Protección cibernética para empresas ofrecido por la CCB , no es seguro que lo sigan ofreciendo, va dirigido a las pequeñas y medianas entidades con el objetivo de que estas se protejan contra amenazas o riesgos cibernéticos, con lo cual lo podrán hacer a sus propios ritmos, manejando los tiempos y curvas de aprendizaje.

Conclusiones

Los delitos informáticos propasan las capacidades de las empresas para proteger su información, ya que los criminales son cada vez más inteligentes y les ayuda la evolución de la tecnología. Las empresas pierden miles de millones de dinero por ser víctimas de este delito, puesto que las pérdidas son grandes, por la evidente adquisición de información por parte de los cibercriminales.

De acuerdo con la información obtenida, la Ciberseguridad no es conocida como debería serlo, puesto que en años anteriores los delitos informáticos no habían tenido un aumento tan significativo, y con la aparición de la pandemia por Covid-19 este se hizo un poco más utilizada, pero no por las personas relacionadas directamente con el manejo de la información.

El tipo de delito informático general de mayor crecimiento en 2020 comparado con el año anterior es la suplantación de sitios web, con 4.776 casos reportados, en comparación a 892 casos en 2019, con un aumento porcentual de 435.

La mayoría de los casos reportados sobre delitos informáticos contra las organizaciones en Colombia es debido a la ingeniería social, que consiste en la manipulación de los usuarios corporativos con el objetivo de tener acceso, permiso o información de sistemas de información, a través de correos falsos y transacciones.

Los programas académicos aquí presentados, tiene cada uno un enfoque diferente, sin embargo, tienen la misma finalidad el de proporcionar herramientas que puedan proteger los sistemas de información como la información misma y que los que la estudien puedan ser de gran importancia para una compañía.

Recomendaciones

Las empresas deberían también enfocarse en herramientas que puedan proteger su información, dedicarles más tiempo, no solamente en cuestiones de tecnología, sino que capacitar a cada uno de sus empleados para así tener mayor probabilidad de no ser víctimas de cibercrimen.

La revisoría fiscal debería plasmar en su legislación, los conocimientos que ayude a fortalecer su plan de trabajo en cualquier empresa dependiendo de las situaciones que sucedan en el mundo que cambie drásticamente el modo de vivir. La ciberseguridad es una de ellas, puesto que proporciona herramientas para proteger la información que el revisor maneja.

Para los siguientes investigadores, hacer una encuesta en donde se plasme preguntas que vallan dirigidas al revisor fiscal o a un contador que esté a punto de ejercer tal cargo, sobre la ciberseguridad, si la maneja, si la empresa en la que está la utiliza, pero si no es así, por medio de esta se daría conocimiento a estos los cuales no saben nada o solo habían oído hablar de esta. Para así guiar esta investigación a un resultado más concreto en donde se identifique que en verdad el revisor implemento la ciberseguridad en su plan de trabajo.

Para los revisores fiscales, los programas aquí presentado cada uno tiene su importancia, pero la Maestría en ciberseguridad y ciberdefensa de la Universidad ESDEG posee un programa más amplio, puesto que contiene conceptos prácticas y procedimientos en cuanto a la seguridad de la información, las telecomunicaciones y el riesgo operacional, en donde los dos últimos no están dentro de los otros planes de estudios de las otras universidades.

Otra maestría podría ser también la del Máster Universitarios de Ciberseguridad y Privacidad de la Universidad Oberta de Catalunya, puesto que ofrece 3 especialidades y abarca diferentes enfoques en cada una de las asignaturas allí presentadas.

Referencias

Argote, C. A. (17 de febrero de 2021). *Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis*. Obtenido de asuntos:legales: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

Banco de la República. (2016). *Riesgo cibernético: relevancia y enfoques para su regulación y supervición*. Obtenido de https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/rref_recuadro_7_2017.pdf

Bermudez, J. M. (2011). *Revisoría Fiscal: una garantía para la empresa, la sociedad y el estado.* Bogotá: Eco Ediciones.

Bodnar, D. (30 de marzo de 2021). *Academy*. Obtenido de Qué es la ingeniería social y cómo evitarla: https://www.avast.com/es-es/c-social-engineering#topic-1

Buitrago, E. R. (20 de enero de 2015). *Repositorio Umng.* Obtenido de La práctica de delitos informáticos en Colombia: https://repository.unimilitar.edu.co/handle/10654/13452

Cámara de Comercio de Bogotá. (2020). *Cámara de Comercio de Bogotá*. Obtenido de Impacto del COVID 19: https://www.ccb.org.co/observatorio/Economia/Economia-dinamica-incluyente-e-innovadora/Impacto-del-COVID-19

Cámara Valencia. (s.f.). *Qué es el hacking ético*. Obtenido de Tecnología para los negocios: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

Código de comercio. (2017). *Decreto 410 de 1971*, artículo 207.

Congreso de Colombia. (05 de enero de 2009). *Ley 1273.* Diario Oficial No. 47.223. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Cruz, Y. E. (15 de septiembre de 2018). Aplicación de los principios de la ciberseguridad como estrategia de continuidad económica en el sector financiero- caso banco de chile y su incidencia en la banca colombiana. Bogotá D.C., Colombia.

El comercio. (27 de enero de 2021). *El coronavirus deja secuelas en los pulmones, corazón y cerebro*. Obtenido de El Comercio: https://www.elcomercio.com/tendencias/covid19-secuelas-pulmones-corazon-cerebro.html

Infosecurity. (s.f.). *Ciberseguridad*. Obtenido de Una guía completa del concepto, tipos, amenazas y estrategias: https://www.infosecuritymexico.com/es/ciberseguridad.html

Jaramillo, L. B. (23 de junio de 2014). El riesgo moral de la revisoría fiscal. Bogotá D.C, Colombia .

Kaspersky. (s.f.). *Latam Kaspersky*. Obtenido de ¿Qué es el ransomware?: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

Melchior, N., & Ducom, I. (s.f.). *Definición y concepto de compliance o cumplimiento normativo*. Obtenido de Mariscal & Abogados - Asociados: https://www.mariscal-abogados.es/definicion-y-concepto-de-compliance-o-cumplimiento-normativo/#:~:text=El%20cumplimiento%20normativo%2C%20conocido%20tambi%C3%A9n,de%20capitales%2C%20etc.).

Organización Mundial de la Salud (OMS). (10 de noviembre de 2020). Obtenido de Información básica sobre la COVID-19: https://www.who.int/es/news-room/q-a-detail/coronavirus-disease-covid-19

Policia Nacional de Colombia. (s.f.). *Denunciar delitos informáticos* . Obtenido de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Prenafeta, J. (23 de agosto de 2018). *Qué es pentesting y cómo detectar y prevenir ciberataques*. Obtenido de Hiberus Blog: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/#:~:text=El%20%E2%80%9Cpentesting%E2%80%9D%20o%20%E2%80%9Ctest,poder%20prevenir%20los%20ataques%20externos.

Tecon. (s.f.). *¿Qué es la ciber-resiliencia*. Obtenido de Blog: Simplificando la tecnología - Tecon: https://www.tecon.es/la-ciber-resliliencia/#:~:text=La%20ciber%2Dresiliencia%20es%20la,desempe%C3%B1o%20general%20de%20la%20empresa.

Venturi, G. (02 de octubre de 2020). *¿Qué es la Criptografía?* Obtenido de Tecnología+Informática: https://www.tecnologia-informatica.com/que-es-la-criptografia/