MÉTODOS PARA DETECTAR, PREVENIR Y CONTROLAR FRAUDES INFORMÁTICOS EN LAS ORGANIZACIONES DEL SECTOR PÚBLICO, PRIVADO Y MIXTO EN COLOMBIA.

CAROL TATIANA GONZÁLEZ BALLESTEROS

Corporación Universitaria Minuto de Dios

Vicerrectoría Tolima y Magdalena Medio

Sede Ibagué

Contaduría Pública

2021, octubre

MÉTODOS PARA DETECTAR, PREVENIR Y CONTROLAR FRAUDES INFORMÁTICOS EN LAS ORGANIZACIONES DEL SECTOR PÚBLICO, PRIVADO Y MIXTO EN COLOMBIA.

CAROL TATIANA GONZÁLEZ BALLESTEROS

Trabajo de grado presentado como requisito para optar al título de

CONTADORA PÚBLICA

Asesor:

Heber Alfredo Guifo Hernández

Contador Público

Corporación Universitaria Minuto de Dios

Vicerrectoría Tolima y Magdalena Medio

Sede Ibagué

Contaduría Pública

2021, octubre

Dedicatoria

Dedico primeramente este trabajo a Dios, porque fue quien puso en mi la sabiduría para sacar adelante no solo este proyecto sino toda mi carrera, a mis padres quienes son los pilares más valiosos en mi vida, pues a lo largo de la suya, han formado un gran ser humano que está a punto de ser una profesional integra con excelente valores y grandes destrezas.

Hoy veo en mí como desde niña me forma con tantas capacidades, con las infinitas bendiciones que Dios puso en mi camino y que nunca me soltó, a pesar de que por el cansancio y demás adversidades de la vida me llevaron a pensar que debía hacer un alto en mi carrera, pero las ganas que desde siempre tuve de ser profesional no me dejaron caer jama.

Agradecimientos

A lo largo de mi carrera encontré grandes personas, docentes y compañeros que ayudaron a forjar en mí, conocimientos que para el día de mañana me harán ser una excelente CONTADORA PUBLICA, con una gran ética profesional que me permitirá ser reconocida por mi trabajo, a ellos también les dedico esta investigación.

En el trascender de mi carrera encontré dos mujeres, excelentes profesionales en todo sentido, siempre creyeron en mí, siempre me motivaban a continuar mi camino, Yaned Patricia y Nury Isabel, dos excelentes cuasi colegas, con unos conocimientos infinitos y una hermosa disposición de trasmitirlos a quienes quieren saber más cada día.

Por último y no menos importante Heber Alfredo Guifo Hernández quien apoyo desde siempre este trabajo, que, aunque en un comienzo no lograba obtener muchos avances, me ayudo con su asesoría a aclarar mis ideas y sacarlo adelante.

Para todos ustedes MUCHAS GRACIAS!

Contenido

Lista de tablas

Lista de figuras

Resumen

El hackeo de la información en las organizaciones ha ido ascendiendo a pasos agigantados en Colombia, esto se debe a que muchas de las empresas no toman controles y precauciones necesarias en el cuidado de la información, pues a esta se permite el acceso de cualquier persona, dejando en riesgo datos confidenciales de los cuales el mal uso puede llevar a una entidad incluso a su pérdida total; es por esto que se debe conocer la importancia y tomar medidas necesarias en cuanto a ciberseguridad, entender e implementar los controles necesarios es de suma importancia pues, a medida que la información es ingresada a la red, las compañías se vuelven mas vulnerables ante los ciberdelincuentes, pues es mucho mas el riesgo de acceso a la misma y desde cualquier lugar, es por esto que poner en marcha salvaguardas y demás para lograr prevenir robos o perdidas de la información debe ser considerado como prioridad; por lo anterior también se requiere de un compromiso por parte de todos los empleados tanto internos como externos que estén involucrados en el acceso a la información, pues muchos de estos accesos forzosos a la información en la mayoría de los casos ocurren porque no se maneja una confidencialidad entre las partes involucradas.

Palabras claves: *Ataque, ciberdelincuente, ciberseguridad, control de seguridad, copia de seguridad, fraudes, hacker, información, phishing, salvaguardas, servidores, suplantación, vishing.*

Abstract

The hacking of information in organizations has been increasing by leaps and bounds in Colombia, this is because many of the companies do not take the necessary controls and precautions in the care of the information, since it is allowed access by anyone, leaving confidential data at risk of which misuse can lead to an entity even to its total loss; That is why it is important to know the importance and take the necessary measures in terms of cybersecurity, understanding and implementing the necessary controls is of utmost importance because, as the information is entered into the network, companies become more vulnerable to cybercriminals. , because the risk of access to it and from anywhere is much higher, that is why putting safeguards and others in place to prevent theft or loss of information should be considered a priority; Therefore, a commitment is also required by all internal and external employees who are involved in access to information, since many of these forced access to information in most cases occur because a confidentiality between the parties involved.

Keywords: *Attack, cybercriminal, cybersecurity, security control, backup, fraud, hacker, information, phishing, safeguards, servers, impersonation, vishing.*

MÉTODOS PARA DETECTAR, PREVENIR Y CONTROLAR FRAUDES INFORMÁTICOS EN LAS ORGANIZACIONES DEL SECTOR PÚBLICO, PRIVADO Y MIXTO EN COLOMBIA.

Introducción.

En el mundo de las organizaciones existe la alta tendencia a considerar solo de alto valor aquellos bienes que son tangibles y altamente avaluados como propiedad planta y equipo, dejando de lado bienes intangibles como lo son las carteras de clientes, patentes, marcas e informaciones y tarifas comerciales, estos elementos anteriormente mencionados constituyen la información de la compañía y debe ser tenido en cuenta como el activo más importante de la empresa.

El avance de la tecnología ha traído consigo una serie de cambios en cuanto a comunicación, procesos, investigaciones, métodos de seguridad, transacciones, entre otros, lo que se presta en la actualidad para que todos aquellos dedicados a realizar comportamientos ilícitos puedan ejercer los denominados “Fraudes informáticos”.

En merito a lo anterior se realiza esta investigación para analizar las formas de trabajo que tienen estos hackers y la labor que se puede realizar en pro de prevenir que sigan realizando este tipo de actos delictivos, lo cual puede generar numerosas pérdidas para las compañías con grandes sumas de dinero en calidad de estafa para poder recuperar la información.

“Colombia no está exenta de este panorama, y así lo muestra el informe del Tanque de Análisis y Creatividad de las TIC (TicTac), en el que se revela que el 2020 fue el año con mayor impacto de ciberataques en Colombia, con más de 45.000 casos denunciados y un incremento del 89 por ciento frente al año anterior.

En este escenario entra el aumento de la conectividad que han experimentado los colombianos en los últimos meses y la poca preparación en cuanto a medidas de seguridad para enfrentar este tipo de amenazas.”

T. (21 de febrero de 2021). Las principales modalidades de ciberdelitos y cómo protegerse. *El tiempo*. Recuperado de https://www.eltiempo.com/

Cifras manejadas por el Centro Cibernético Policial muestran que el cibercrimen ha tenido un crecimiento cercano al 40% en los últimos años.

La ley 1273 de 2009 o ley de delitos informáticos contempló como bien jurídico tutelado la protección de la información y los datos.

En dicha norma se encuentran tipificados nueve delitos que van dirigidos a la protección de la información, los datos y el patrimonio económico.

Marco referencial.

- Marco teórico y conceptual.

Los delitos informáticos son los actos ilícitos que se cometen a través de espacios digitales, entornos digitales o en internet. En Colombia puede definirse que los delitos informáticos son los accesos de manera ilícita o no autorizada a los datos e información que están resguardados en formatos digitales.

Sujetos de los delitos informáticos

Sujeto activo: De acuerdo al profesor chileno Mario Garrido Montt, (Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992).se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal. Las personas que cometen los “Delitos Informáticos” son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el

manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Sujeto pasivo: El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros. El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Clasificación de los delitos informáticos

Para poder crear sistemas de protección y seguridad informática, es muy importante conocer los delitos informáticos más comunes. La importancia de ello es prevenir víctimas, que para este caso son organizaciones ubicadas dentro del sector público y privado, se puede observar que los siguientes delitos informáticos son los más comunes.

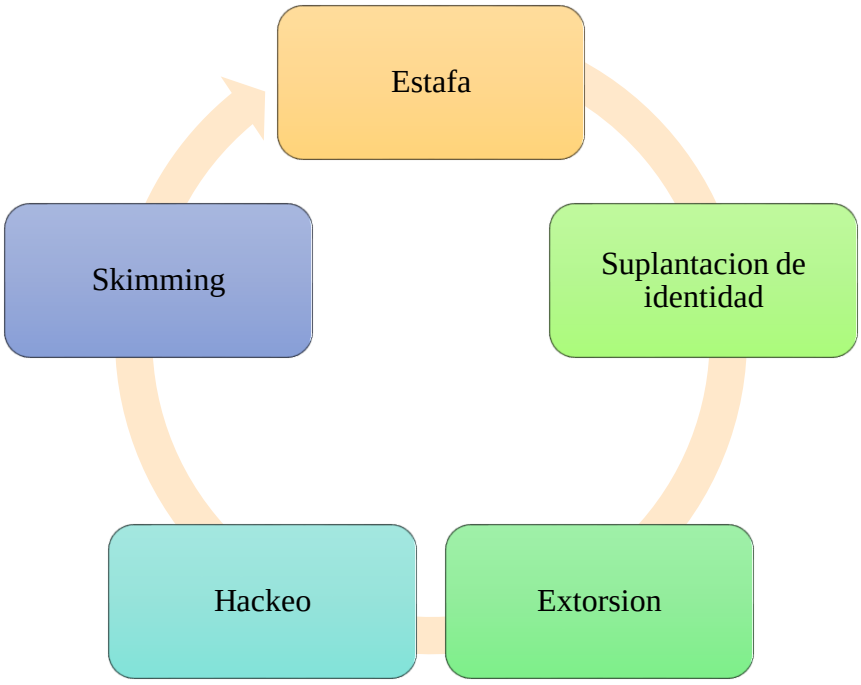


Figura 1.
Clasificación de delitos informáticos.
Elaboración propia.

- Estafa: Este tipo de delito se comete a través del robo de identidad. Los criminales utilizan técnicas como el spam, webs falsas o software ilegales para engañar a las víctimas y robarles las contraseñas o claves personales. De esta manera, acceden a información confidencial. Un ejemplo de ello es el acceso a datos bancarios.
- Suplantación de identidad: Relacionado con lo anterior, la suplantación de identidad sucede cuando la estafa tiene éxito y el criminal obtiene acceso a la información personal. Una vez obtenida, el criminal puede realizar compras, llegando a arruinar a la víctima, o hacerse pasar por la persona a quien ha robado los datos.
- Extorsión: Este delito sucede cuando alguien utiliza internet para extorsionar dinero a una persona o empresa. La extorsión se comete de distintas formas. Por ejemplo, el criminal puede tener acceso a información personal y amenazar con exponerla a menos que pague cierta cantidad de dinero a cambio. Los delincuentes también pueden llevar a cabo algún tipo de ataque

cibernético para luego exigir un pago para detenerlo. Por este motivo, es muy importante tener un antivirus y proteger las cuentas bancarias y personales con contraseñas de alta dificultad.

- Hackeo: Este delito se considera muy grave, ya que el hacker intenta obtener acceso a cuentas personales con la ayuda de un ordenador. Con ello consigue robar información confidencial y puede llegar afectar a los negocios de una empresa.
- Skimming: consiste en el copiado de la banda magnética de una tarjeta (crédito, débito), este acto delincuencial hace referencia al robo de información de tarjetas de crédito utilizado en el momento de la transacción; su finalidad es clonar las tarjetas de crédito o débito para proceder con la artimaña de reproducción ilegal.

Los ambientes más propicios donde el Skimming se puede emplear de una manera exitosa, son los cajeros electrónicos, bares, gasolineras y restaurantes; ya que este método se puede ejecutar solamente instalando un dispositivo que logra copiar la información de la tarjeta.

Control de acceso a la información

Por defecto, toda organización debe seguir el principio del mínimo privilegio. Este principio se traduce en que un usuario sólo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones diarias. Para conseguir este objetivo, previo a la implementación de medidas técnicas o salvaguardas, debemos realizar los siguientes pasos:

1. Definir los diferentes tipos de información que existen en nuestra organización: datos de recursos humanos, contabilidad, clientes, marketing, producción, etc.

2. Establecer quién puede acceder a cada tipo de información. Para acometer esta tarea puede ser útil, si la estructura organizativa lo permite, realizar una matriz que cruce información con áreas o departamentos que tienen necesidad de acceso a dicha información.

El control de acceso debe ser concedido de acuerdo con quién necesita saber, quién necesita usar y a cuánto acceso requieren. Los controles de acceso según ISO 27001 pueden ser de naturaleza digital y física: por ejemplo, restricciones de permisos en las cuentas de usuario, así como limitaciones sobre quién puede acceder a ciertas ubicaciones físicas.

Ciberseguridad en Colombia

La suplantación de sitios web y robo de datos están entre los delitos más frecuentes y denunciados.

La llegada del covid-19 no supuso solamente un cambio en las pautas de salud, sino también una nueva forma de interacción con las plataformas digitales tanto para empresas como para los ciudadanos.

Con esa llegada de la virtualidad todos nos volvimos más vulnerables ante las operaciones, transacciones y trámites que hacemos desde un computador o un teléfono móvil. Por ejemplo, tan solo en el primer trimestre de 2020, un periodo difícil por causa del confinamiento, los ciberdelitos aumentaron 37% comparado con 2019.

Uno de los sucesos más recientes ocasionado por los ciberdelincuentes, es el caso de fraude y ciberseguridad por el que paso la reconocida entidad bancaria Banco Davivienda, pues no tomando los controles necesarios y realizando una mínima verificación en la titularidad de sus clientes realizaron desembolsos de créditos y aprobación de pagos mediante compras virtuales, de las cuales los titulares nunca dieron autorización, esta es la versión entregada por esta entidad.

“Se realiza permanentemente la adopción de buenas prácticas en seguridad de la información, la atención y respuesta a los diferentes requerimientos de los entes reguladores, la participación activa en diferentes mesas de trabajo sectoriales con autoridades, la actualización

continua de modalidades de fraude y de las herramientas que permiten proteger a los clientes ante posibles eventos de fraude”

Por otro lado también señalo que “cuenta y continúa su esfuerzo por obtener las mejores tecnologías para la prevención del fraude y protección de nuestros clientes y realiza permanentemente campañas de comunicación y educación de prevención”.

P (07 de octubre de 2021). Davivienda se pronuncia sobre casos de fraude y ciberseguridad. *Portafolio.* Recuperado de https://www.portafolio.co/

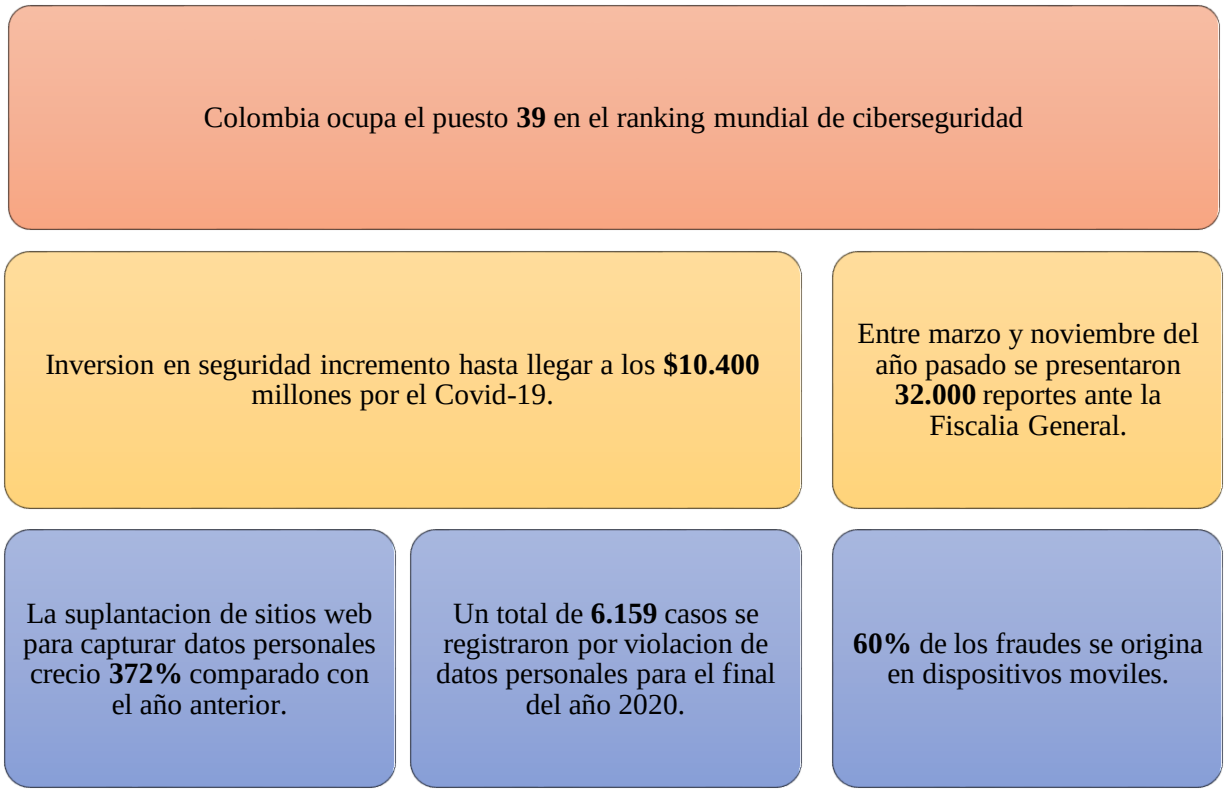


Figura 2.
Incrementos de Ciberdelitos en Colombia.
Elaboración propia.

Según la estadística entrega por Cristian Acosta Argote, dentro de la página asunto:legales se conoce que para ese mismo lapso de tiempo, se registraron 7.082 denuncias, lo

cual representó un incremento de 27%, según datos de la Cámara Colombiana de Informática y Telecomunicaciones.

A pesar de la reactivación económica y el fin de la cuarentena generalizada, para noviembre de 2020 hubo un aumento de 83% de los delitos cometidos por medios informáticos, pues se pasó de 21.107 en 2019 a 36.834 delitos.

Entidades Gubernamentales más suplantadas en Colombia

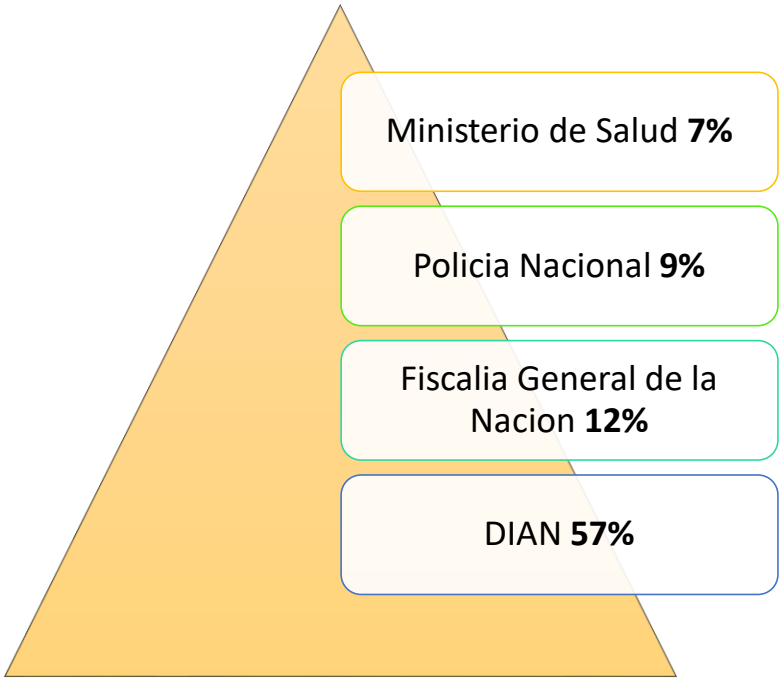


Figura 3.
Entidades Gubernamentales más suplantadas en Colombia.
Elaboración propia.

Incremento de los delitos en Colombia

Modalidad	2019	2020	Variación
Correo electrónico Spam y Scam	4	41	925%
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 correos ajenos	333	1527	359%
Introducción a extraer del país software malicioso	4	17	325%
Simulación de App Móvil	58	238	310%
Suplantación de blog	2	8	300%
Ingeniería social	107	427	299%
Captura de tramas de red de computadores	15	56	273%

Tabla 1.
Delitos que más crecieron.
Elaboración propia.

- Marco legal.

LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

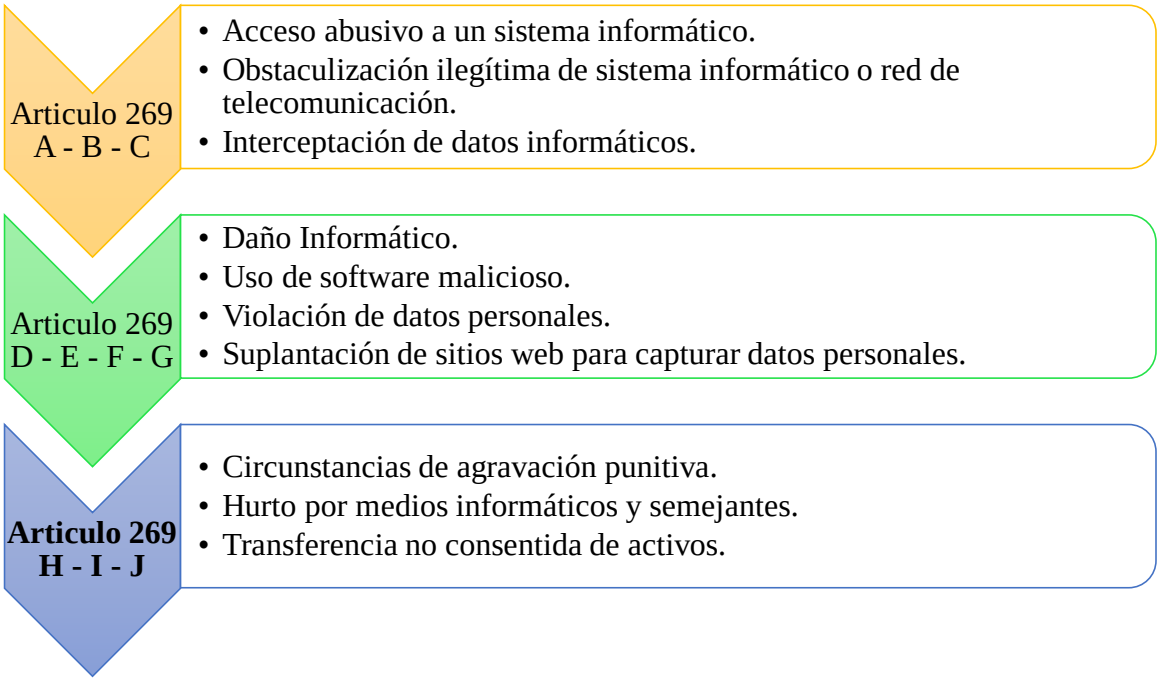


Figura 4.
Artículos de la Ley 1273 de 2009.
Elaboración propia.

Por otro lado el desconocimiento de las normas no exculpa a una persona de haber cometido un delito informático, esto debido a que el Estado Colombiano presume que sus ciudadanos conocen las leyes. La pena mínima impuesta por un cargo de delito informático es de 4 años, y además para este tipo de delitos no es posible modificar la medida de aseguramiento, es decir no se puede solicitar privilegio alguno.

En Colombia durante el último trimestre y en medio de la cuarentena por Covid-19 se han incrementado casi en un 55% los casos de denuncia por delitos informáticos, por estafa y robos a través de servicios de redes, por ello La Fiscalía habilitó la línea 122 para denunciar este tipo de crímenes, además que muchas entidades financieras están desarrollando y creando mecanismos de seguridad para sus usuarios. Si es usted víctima de un delito informático, diríjase de inmediato a la Policía Nacional o Fiscalía General de la nación. Según lo referencia la reconocida firma de abogados World Legal Corporation expertos en delitos informáticos.

Penas de prisión, que van desde los 48 a los 96 meses, tendrán que pagar quienes cometan estas infracciones.

También recibirán multas de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Justificación

El presente proyecto nos permitirá trabajar sobre los diferentes métodos para detectar, prevenir y controlar fraudes informáticos, los cuales ayudarán a que las empresas conozcan la importancia que tiene la información en sistemas y que por desconocimiento de los mismos se podrían ver expuestos al robo (hackeo) de la información, no solo de sistemas privados de la empresa, sino también a sus páginas web o programas de manejo online.

Teniendo en cuenta lo anterior, si no se manejan las estrategias necesarias y no se implementan sistemas de control, los ciberdelincuentes podrían extorsionar a las organizaciones y solicitar a cambio altas sumas de dinero por la devolución de la información, información que en la mayoría de los casos solo le servirá a la propia compañía.

Además de la dos estrategia más conocidas para salvaguardar la información, como lo son, el no guardar contraseñas en equipos extraños a los frecuentemente utilizados y no permitir la exportación de archivos, se debe tener en cuenta la importancia del uso de la copia de seguridad en un disco externo el cual salvaguarde todo tipo de información.

También debemos tener en cuenta que la adopción de un determinado control para mejorar la seguridad en una dimensión, puede afectar de forma negativa o positiva a otra de las dimensiones, por ello, es esencial conocer cuál de estas dimensiones es más importante proteger en cada sistema de información. Por ejemplo, implantar un control de acceso para proteger la confidencialidad de la información contable y financiera de cualquier tipo de empresa.

Definición del problema

Para el hackeo de la información hoy por hoy existe una amplia variedad de metodologías utilizadas por los ciberdelincuentes mediante las cuales se puede ejecutar el robo de la información, pues las memorias USB o discos duros facilitan el rápido almacenamiento de la información por medio de la exportación de la misma, teniendo en cuenta que para la mayoría de ocasiones no se tiene autorización de ejecutar dicho proceso que para cualquiera de las entidades bien sea del sector público o privado es un inminente riesgo.

Por otro lado también se tiene el riesgo de la exportación y envió de información mediante correo electrónico convencional o la encriptación de la misma por medio de virus que llegan al correo electrónico personal o corporativo de la organización, como también la descarga de

cualquier tipo de información permitiendo así el acceso de virus que posteriormente toman la información haciendo uso delincuencial de esta.

Para cualquier tipo de compañía se deben tener en cuenta los principales errores que se cometen, pero también por otro lado el uso adecuado de algunas herramientas que minimizan el riesgo.

ERRORES	MEDIDAS
Información importante de la que no se realiza copia de seguridad.	Para evitar cometer este error tendremos que asegurarnos que tenemos una copia de seguridad actualizada de la información, al menos de aquella más crítica. Y comprobaremos que sabemos y que podemos recuperarla.
Carpetas de red compartidas sin control de acceso. Usuarios que no saben dónde está la última versión de un documento. Usuarios que tras un cambio de puesto conservan acceso a información que, por el nuevo tipo de trabajo que van a desempeñar, no es necesaria.	Estos errores se pueden evitar si hacemos que la información sólo sea accesible a quien la necesita y esté autorizado para ello. Es decir implantar un «control de accesos».

Presencia de discos duros portátiles sin que la organización conozca y tenga inventariados quién los utiliza y qué información pueden tener almacenada. Falta de formación de los usuarios en las herramientas que utilizan. Dejar que los empleados utilicen almacenamiento en la nube y su correo personal para actividades profesionales.	Si no se limita el uso de aplicaciones no corporativas (correo personal, almacenamiento en la nube) y se controla el uso de los dispositivos externos ni los usuarios tienen la adecuada formación, cometeremos estos errores.
Tirar los ordenadores y discos a la basura sin ningún control previo de su contenido.	Tener controlados los soportes y los equipos es esencial pues algún día dejan de ser útiles, por obsoletos o por desgaste. Es el momento de deshacerse de ellos, borrar toda la información que tenían, de forma que no quede ni rastro de su uso previo.

Tabla 2.
Errores más comunes en el tratamiento de la información en la empresa.
Tomado de: INCIBE

El adecuado uso de la tecnología es vital para la funcionalidad en cualquiera de los departamentos de las organizaciones, pues al implementar medidas para minimizar el riesgo de fraude se incrementa la seguridad en la información y el hecho de conservarla sin que ningún delincuente afecte la productividad en el transigir de las operaciones.

Objetivos

Objetivo general

Analizar los diferentes métodos para detectar, prevenir y controlar fraudes informáticos en las organizaciones del sector público, privado y mixto en Colombia.

Objetivos específicos

- Identificar los métodos informáticos de fraudes en las organizaciones del sector público y privado.
- Evaluar los distintos riesgos a los que se encuentran expuestos las empresas y organizaciones.
- Proponer controles para conservar la confidencialidad y la seguridad de la información.

Diseño metodológico

- Método o estructura de unidad de análisis

Como eje principal de la investigación se manejan las estructuras de fraude dentro de las organizaciones de orden público y privado las cuales comprenden los sectores económicos relacionados a continuación.

Teniendo en cuenta lo anterior, para estas organizaciones los mecanismos de ciberseguridad son un flagelo muy grande, pues estas en su mayoría no tienen salvaguardas de mucha seguridad que permita minimizar riesgos ante el robo de información.

Figura 5.
Sectores económicos con mayor riesgo.
Elaboración propia.

En cuanto a la selección de salvaguardas de información en cualquiera de las organizaciones se tienen en cuenta puntos importantes para la selección de estas, por ejemplo:

1. Sector de negocio → Importancia de la información de la empresa
2. Identificar, valorar y clasificar la información → Confidencial, interna o pública.
3. Conocer la naturaleza de los controles → Técnica (medida de carácter tecnológico), organizativa (formación de seguridad, identificación de responsables o implantación de procedimientos) y física (acondicionamiento de sala de servidores, cámaras y demás mecanismos que prevean el acceso inadecuado a la información)
4. Costo de las medidas = Proporcional al riesgo → Costo de tiempo, económico y de recursos humanos empleados para tomar dichas medidas.

La asignación de permisos sobre los recursos que contienen la información puede realizarse individualmente, por perfiles o por grupos de usuarios. Tanto los sistemas Windows

como los sistemas basados en Unix permiten asignar este tipo de permisos, de manera que se optimice su gestión.

- Criterios, validez y confiabilidad
  - Sector financiero: Se maneja información confidencial tanto de clientes como de operaciones financieras de compras y ventas de activos cuya difusión puede suponer una importante pérdida económica o un perjuicio para los clientes.

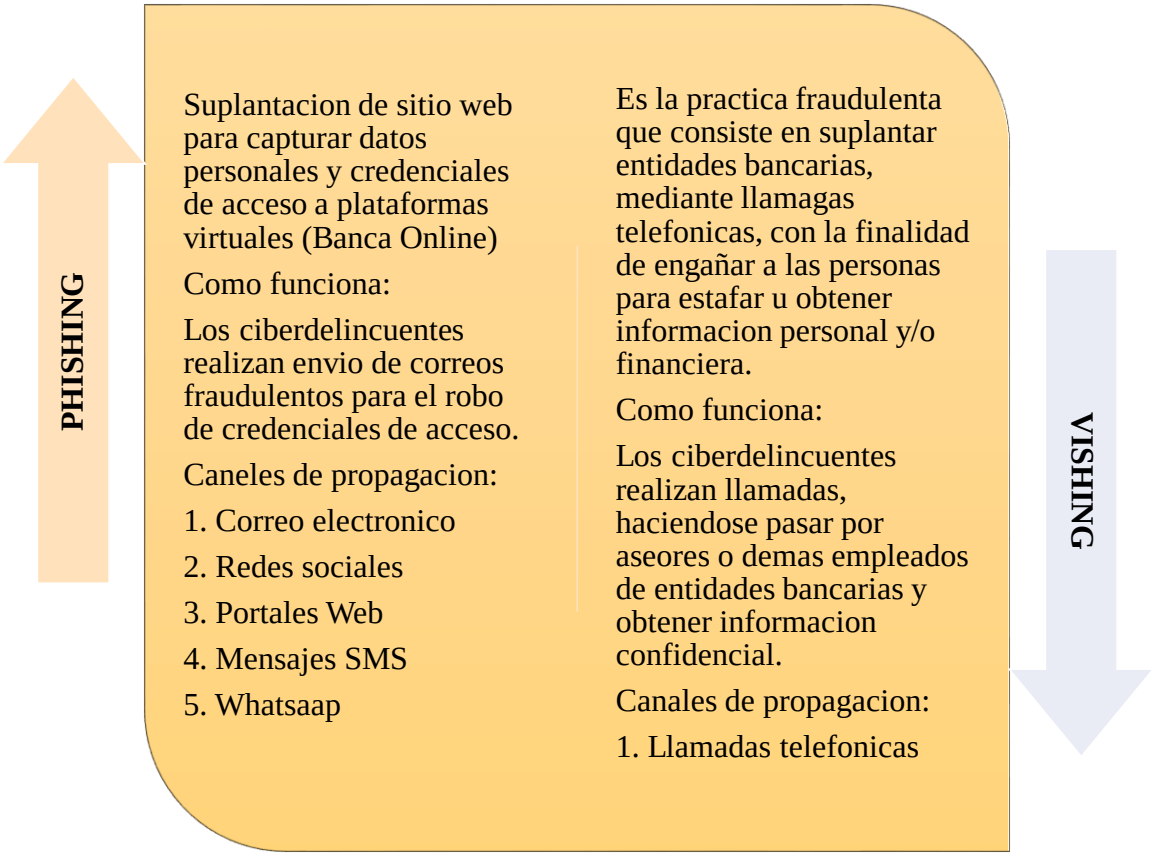


Figura 6
Modus operandi, entidades financieras.
Elaboración propia.

Estadísticas:

Según las bases de datos del Centro Cibernético Policial – Policía Nacional de Colombia. El ciberdelito financiero obtuvo un total de 40.712 denuncias para el año 2020, de las cuales el 2.8% (1.140) de estas se logró captura.

En cuanto a inversiones de ciberseguridad esta tuvo incremento en cifras expresada en millones de la siguiente forma:

2018 → $80.000

2019 → 192.000

2020 → 315.000

"Así, de acuerdo con el presidente de Asobancaria, Hernando José Gómez, el presupuesto destinado a la seguridad digital por parte del sector creció un 64% entre 2019 y 2020, pasando de $192.000 millones a $315.000 millones.

Estos recursos fueron invertidos principalmente en el robustecimiento de las plataformas y medios tecnológicos de las entidades financieras y pago de servicios especializados de soporte de seguridad."

P (01 de julio de 2021). Bancos aumentaron 64% gastos en ciberseguridad. *Portafolio*. Recuperado de https://www.portafolio.co/

Recomendaciones:

1. Cambio de contraseñas periódicamente.
2. Utilizar combinaciones alfanuméricas.
3. No utilizar fechas de nacimiento, nombres de personas o mascotas.
4. No utilizar la misma contraseña en diferentes cuentas.

5. Añada barreras sobre las mismas (* / # $ % &)

- Sector industrial: Es importante velar por la confidencialidad de los procesos y procedimientos que nos pueden aportar una mejora de productividad sobre la competencia.

Estadísticas:

Colombia cuenta con diversos organismos públicos nacionales que velan por generar un marco legal adecuado, que garantice la progresiva incorporación de la ciberseguridad industrial en las estructuras de las empresas con presencia nacional (principalmente infraestructuras críticas), entre las principales cabe destacar:

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT
- Comando Conjunto Cibernético – CCOC
- Centro Cibernético Policial – CCP
- MINTICS
- Ministerio de Defensa Nacional

A continuación, se describe el nivel de sensibilidad de las organizaciones industriales en Colombia, cifras expresadas en porcentajes.

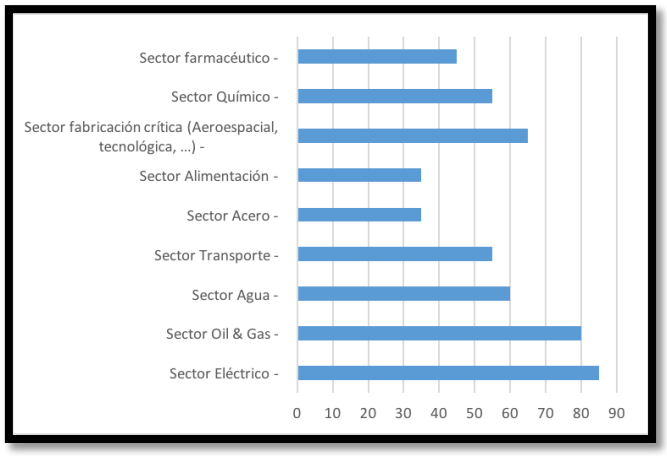
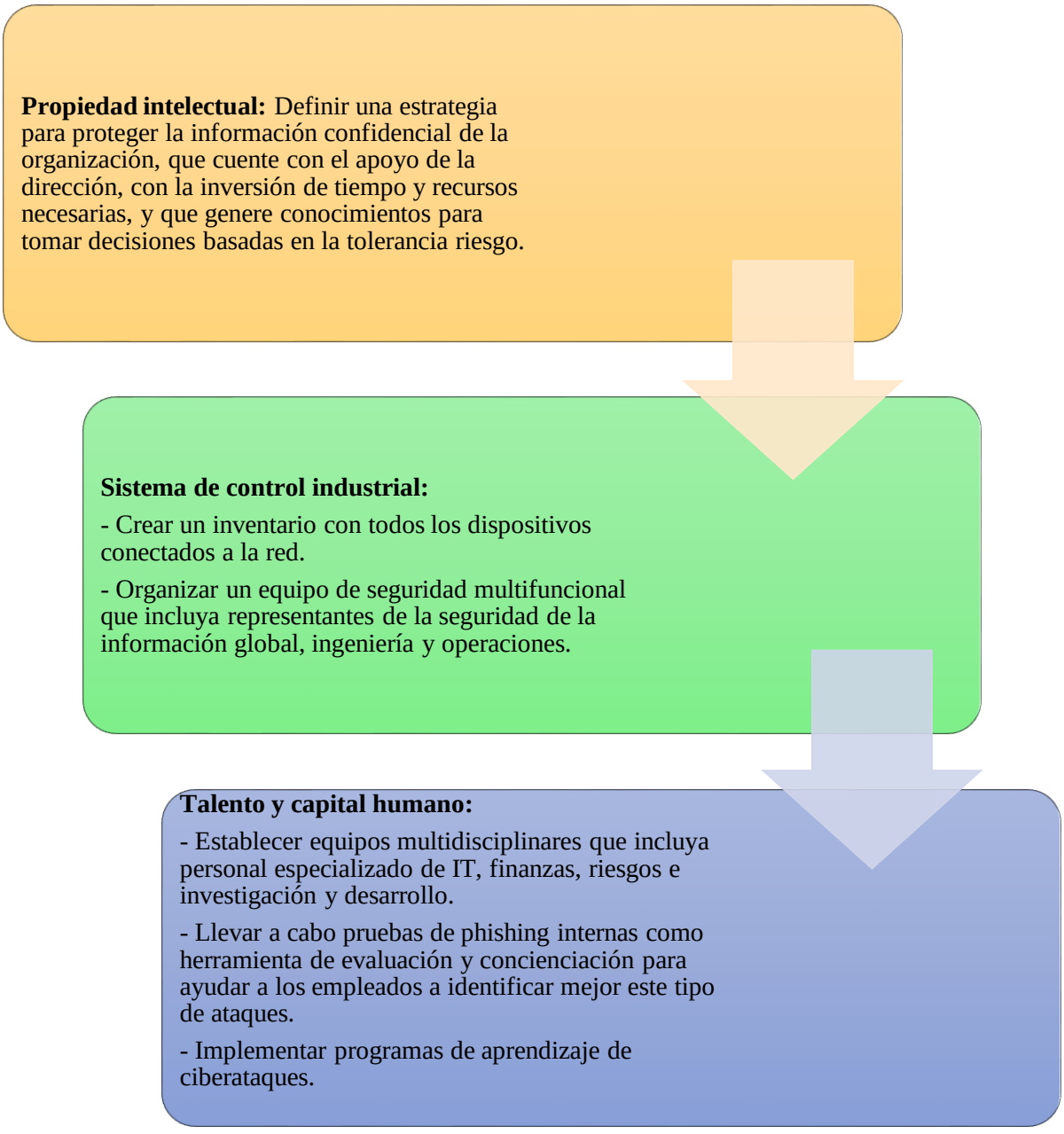


Figura 7.

Nota. Adaptado de La Ciberseguridad Industrial en Colombia, de Diego Andrés Zuluaga Urrea y Claudio Caracciolo, 2021, https://www.cci-es.org/maps/colombia/

Recomendaciones:



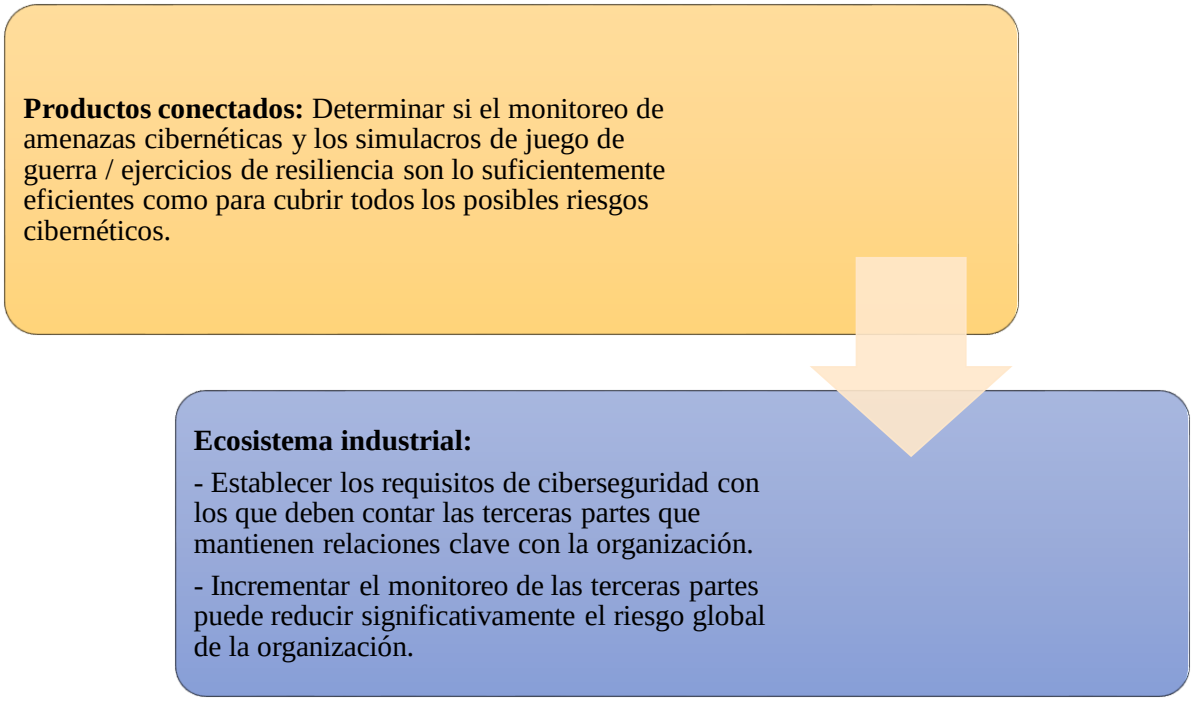


Figura 8.
Recomendaciones de ciberseguridad para el sector industrial.
Elaboración propia.

- Sector Educativo: Las instituciones educativas manejan grandes volúmenes de datos personales de alumnos y del equipo docente, pero también documentos de identidad, datos financieros, historial académico, registros médicos, por lo que se convierten en un blanco estratégico de los ciberdelincuentes para afectar la privacidad de las personas y sobre todo la integridad de la información.

Los ciberataques a las instituciones educativas cada vez se vuelven más frecuentes. En cualquier etapa académica, los alumnos recurren a sus teléfonos inteligentes, tabletas y portátiles para acceder a información y reforzar conocimientos.

Sin embargo, en caso de que algún agente malicioso llegase a infiltrarse o hackear el equipo de algún alumno o profesor, las redes y sistemas educativos de la institución podrían

verse expuestos, con resultados fatales, debido a que por lo general manejan información muy sensible.

En ese sentido, hoy en día los centros educativos de todo el mundo se están dando cuenta de la necesidad de asegurar los equipos de sus estudiantes y colaboradores.

Estadísticas:

Según el informe de filtraciones de datos de 2020, en ese año se presentaron 819 incidentes, de los cuales el 67% de las infracciones fueron causadas por personas externas; 92% de las infracciones fueron motivadas económicamente; 75% de los datos comprometidos eran personales; 80% de los incidentes de malware se pueden atribuir a ransomware.

Recomendaciones:

- Contar con una solución antivirus que cuente con capacidades de cifrado, backup, y doble factor de autenticación para acceder a las diferentes cuentas.
- Actualizaciones, manteniendo al día todos los sistemas.

- Capacitación y concientización sobre lo elemental en seguridad informática (por ejemplo, contraseñas seguras) y sobre temáticas como cyberbullying o grooming.
- Auditorías para conocer el estado de la seguridad, evitar brechas, actualizar permisos de administradores, entre otros

Figura 9.
Recomendaciones de ciberseguridad para el sector educativo
Elaboración propia.

- Gobierno: El Ciberespacio está considerado como un nuevo campo de batalla para el que todos los países, incluyendo Colombia, deben capacitarse para defenderse de posibles ataques cibernéticos.

Sin embargo, muchos todavía luchan por obtener recursos para iniciativas de ciberseguridad y encontrar talento calificado. Para ayudar a enfrentar estos desafíos, los CISO gubernamentales pueden aprovechar su mayor visibilidad e influencia para:

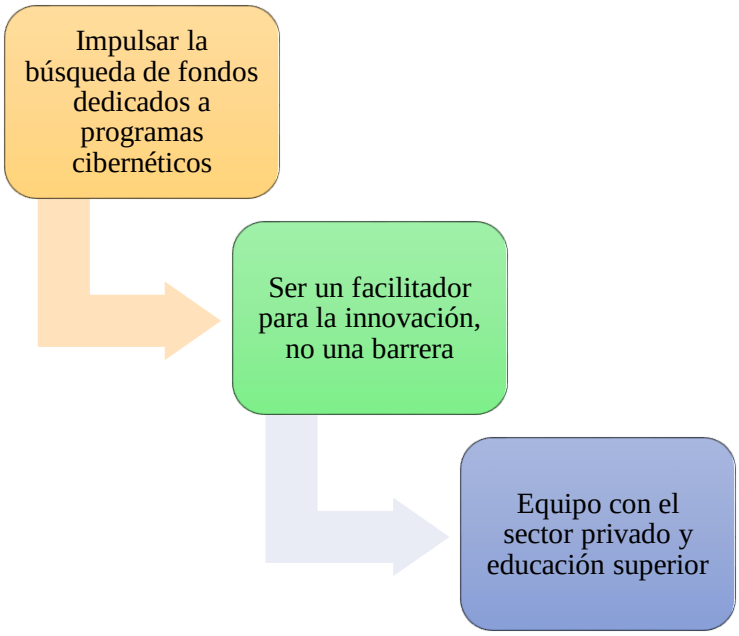


Figura 10.
Iniciativas de ciberseguridad para entidades del Gobierno Colombiano.
Elaboración propia.

Estadísticas:

Los fraudes por canales digitales, delito que en 2020 registró un aumento del 44 % y en el que las alcaldías y gobernaciones presentaron pérdidas por $50.000 millones; el phishing, seguridad de la información, ataques y delitos informáticos, riesgos de navegar en el ciberespacio, fraudes bancarios, manejo de contraseñas y protección de equipos, entre otros, son

el que el Ministerio de las TIC y Asobancaria consideran más recurrentes en cuanto a fraudes informáticos.

Hernando José Gómez, presidente de Asobancaria, sostuvo que el desconocimiento de las medidas de seguridad en el uso de los canales digitales es la causa más común de fraude virtual.

Según cifras de la Fiscalía General de la Nación, entre marzo y noviembre de 2020 se reportaron a esta entidad más de 32.000 denuncias relacionadas con ciberataque; de estas, 12.000 fueron de hurto por medios informáticos.

Entre las entidades gubernamentales las más afectadas por estos ciberdelincuentes fueron, La Administración de Impuestos y Aduanas, La Registraduria Nacional del Estado Civil, La Fiscalía General de la Nación y las Autoridades de Transito.

Recomendaciones:

- Implemente una solución que le permita investigar rápidamente cualquier actividad sospechosa y altamente maliciosa.
- Evaluar y analizar las necesidades que tienen como entidad estatal para poder adoptar una herramienta tecnológica que sea óptima.
- Adoptar las mejores prácticas de ciberseguridad; incrementando la forma de validar la identidad a través de múltiples factores de autenticación. Esto ayudará a establecer políticas de seguridad mucho más seguras definiendo que tipos de dispositivos se pueden conectar a la red y acceder a la información.

- PYMES: El 60 % de las pequeñas y medianas empresas en Colombia no pueden sostener sus negocios luego de sufrir un ciberataque o ataque informático, según revela el Informe de Tendencias del Cibercrimen en Colombia (2019-2020).

Sin embargo, una pyme que no cuenta con estas herramientas de ciberseguridad incrementa sus riesgos de ser atacadas por la cribercriminalidad. Puede sufrir afectaciones económicas, pérdida de información y de reputación que la podrían llevar a la quiebra. Por eso proteger los activos de la empresa debe ser prioridad si se quiere triunfar en las dinámicas de mercado que se imponen y que exigen el uso del internet y la tecnología.

Estadísticas:

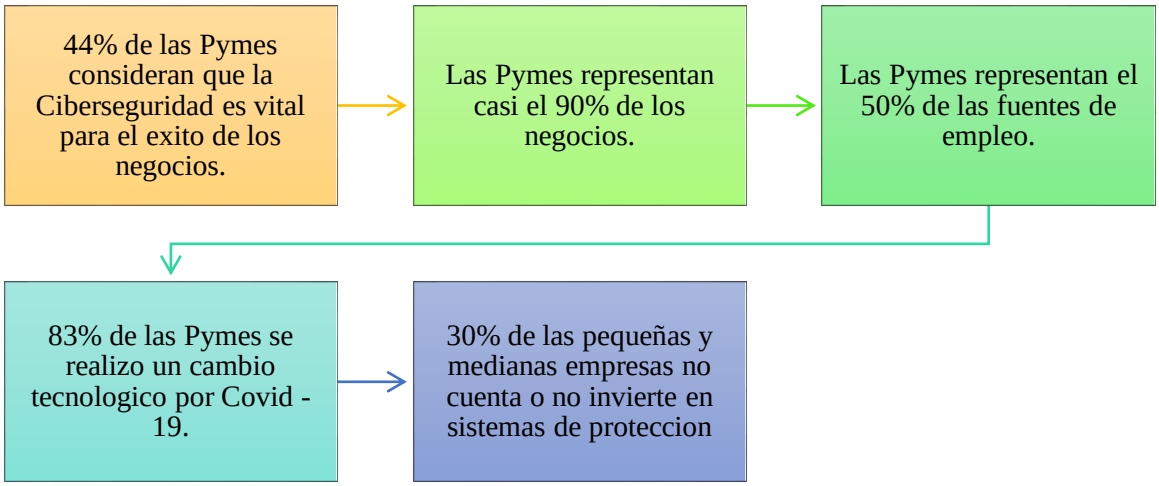


Figura 11.
Estadísticas de ciberseguridad Pymes.
Elaboración propia.

Por cuenta del teletrabajo y la mayor digitalización que creó la pandemia, los ciberataques se han incrementado. Solo en Colombia, en algunos momentos el crecimiento de estos fue de 300%.

En Colombia, de acuerdo con el Centro Cibernético Policial (CCP), el 87% de las empresas víctimas de incidentes digitales no denuncian los ataques. Los sufren por falta de programas de prevención, pues es reconocida la baja inversión en tecnologías para frenar este tipo de incidentes.

Recomendaciones:

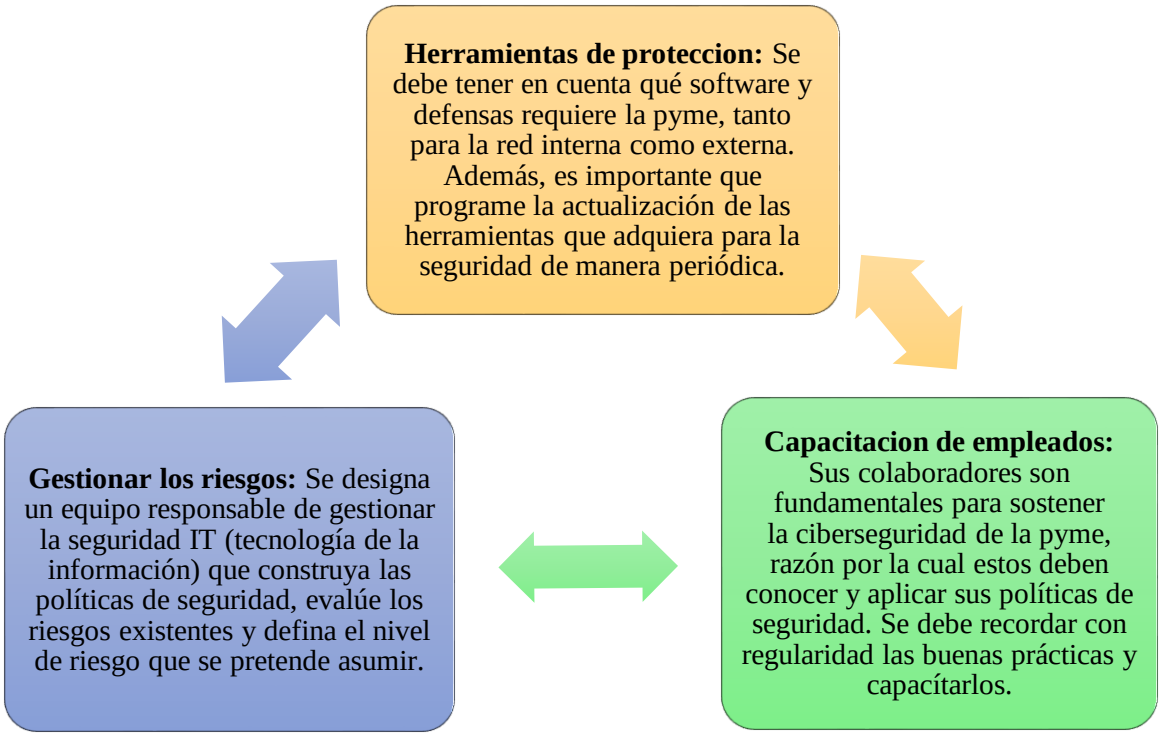


Figura 12.
Recomendaciones de ciberseguridad en Pymes.
Elaboración propia.

Aprender a gestionar la seguridad de las empresas permite prevenir y minimizar el riesgo de un ciberataque. Si bien no existe una fórmula que lo blinde, se pueden emplear cualquiera de estas acciones anteriormente mencionadas.

Según el Ministerio de Tecnologías de la Información y las Comunicaciones, para mantener la seguridad de la información, cada entidad debe velar porque el modelo de gestión de seguridad de la información genere un valor agregado, representado en niveles de riesgos a un nivel aceptable y a un costo razonable. La Unidad de TIC de la entidad debe identificar los riesgos, elaborar el mapa de riesgos y gestionar los mismos, basados en el apetito del riesgo definido por el gobierno del negocio, teniendo en cuenta que se debe velar por el manejo y cumplimiento del mismo.

- Definición de hipótesis

Ante la frecuente amenaza que maneja cualquiera de las entidades bien sea del sector público, privado o mixto; esta se evidencia en que el mayor valor pesa sobre el desconocimiento en cuanto a la ciberseguridad, según los medios de comunicación, hay una generación preparada para ello, la llamada generación digital o nativos digitales, personas encargadas del diseño, implementación y manejo de sistemas que permiten salvaguardar la información sensible al robo por parte de los ciberdelincuentes, es por esto que se ha diseñado en esta investigación un pregunta que abarca todo en cuanto al riesgo de la organizaciones.

¿Qué conocimiento en ciberseguridad tienen las organizaciones y de cuanto es el riesgo que corren al no tomar las medidas necesarias?

Resultados

Teniendo en cuenta todo lo que con anterioridad se ha investigado y plasmado en el presente trabajo, se puede concluir que lo más importante para cualquiera de la organizaciones sin importar el sector económico al que pertenezcan, es la protección de toda su información,

bases de datos y demás que puedan ser susceptibles al hurto, daño y otros cuales sean necesarios proteger de los ataques por parte de los ciberdelincuentes.

Toda entidad debe tener claro que para la protección de su información existen tres dimensiones para salvaguardar su activo más importante.

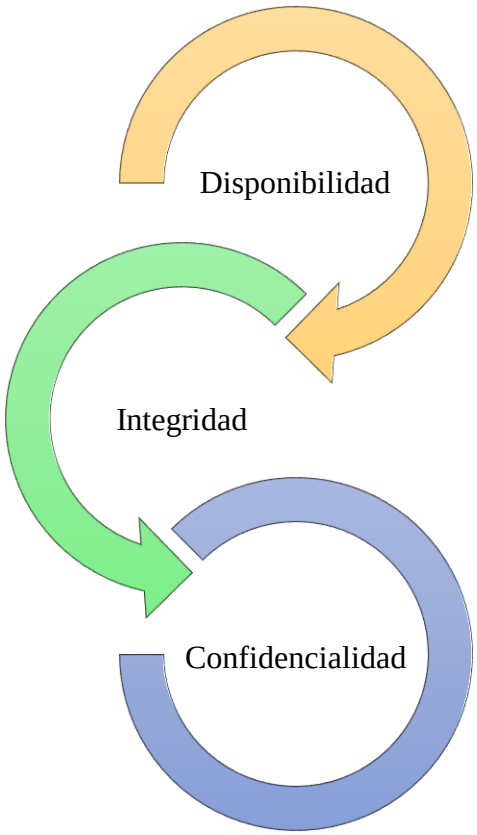


Figura 13.
Dimensiones de la seguridad de la información.
Elaboración propia.

Disponibilidad: Hace referencia a que la información esté accesible cuando se necesite.

Integridad: Se refiere a que la información sea correcta y esté libre de modificaciones y errores.

Confidencialidad: Implica que la información es accesible únicamente por el personal autorizado.

Otro aspecto importante a considerar en la selección e implantación de controles es su tipología o naturaleza.

1. Técnica: Medidas que hacen énfasis en mejoras de carácter tecnológico dentro del ámbito de la seguridad. Son medidas técnicas un antivirus, un cortafuego o un sistema de copias de seguridad.
2. Organizativa: Medidas que se centran en la mejora de la seguridad tomando en cuenta el impacto de las personas. En este caso podemos encontrar la formación en seguridad o la implantación de procedimientos formales de alta y baja de usuarios.
3. Física: Medidas físicas para proteger la organización. Como por ejemplo, acondicionar adecuadamente la sala de servidores frente a riesgos de incendio, inundaciones o accesos no autorizados, establecer un sistema de control de acceso para entrar en las oficinas, poner cerraduras en los despachos y armarios o guardar las copias de seguridad en una caja ignífuga.
4. Legal: Medidas que buscan el cumplimiento legal al que está sujeta la organización en el ámbito de la seguridad de la información. Por ejemplo, medidas de seguridad requeridas por la LOPD, que pueden ser técnicas, organizativas y/o físicas.

Para Adriana Ceballos, directora de desarrollo de programas del Tanque de Análisis y Creatividad de las Tic (TicTac) “La ciberseguridad es el área que mayor atención deberá tener en el 2021, pues un gran número de colaboradores seguirán operando desde sus hogares” además agregó que “el nuevo documento construido por el programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), llamado ciberseguridad en entornos cotidianos, en el que participó Claro, es precisamente, el análisis de diferentes contextos como, trabajo remoto,

ciberseguridad en dispositivos móviles, ciberataques a correos electrónicos, entre otros, donde hoy en día es más necesario implementar políticas robustas de ciberseguridad".

Según lo establece el informe de tendencias del cibercrimen emitido por la Cámara Colombiana de Informática y Telecomunicaciones, la concentración del fenómeno criminal en 2019 - 2020 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados.

Es por todo lo anterior que se debe conocer la importancia que tiene implementar un buen sistema que permita salvaguardar todo tipo de información y de esta forma minimizar lo más que se pueda el sabotaje, robo y mal uso de la información; teniendo en cuenta que cualquiera de los factores mencionados anteriormente y el paso desapercibido en cualquiera de las recomendaciones, puede llevar a cualquier empresa hasta la pérdida total.

En Colombia, si miramos de cerca las amenazas cibernéticas y lo que han hecho las empresas para mitigar el impacto de los ciberataques, surgen cuatro escenarios a analizar: empresas que implementan políticas internas, empresas que actualizan su normatividad interna, empresas que aplican medidas técnicas y empresas que crean estándares digitales.

Para hacer frente a estos ciberataques, las empresas colombianas comenzaron a capacitar a las personas, investigar las fuentes de estas ciberamenazas y crear pequeñas startups para aprender a lidiar con esto y brindar soluciones para empresas nacionales e internacionales.

Empresas dedicadas a brindar ciberseguridad en Colombia:

- PSL Corp.
- BairesDev
- Gorilla Logic
- Tudip Technologies
- GRUPO ORUSS

- Fluid Attacks
- MAS Global Consulting
- Wolox
- Onward Development
- Leanware
- Paradiso
- MQA AMERICAS
- iSy TEk
- TICS SAS
- Software Dexon
- Junpack
- 2Secure SAS

Referencias

- ✓ Analitik, V. (2021, 27 febrero). Actividad maliciosa en internet aumentó en un 150 % en Colombia durante aislamiento. Valora Analitik. https://www.valoraanalitik.com/2021/02/27/actividad-maliciosa-en-internet-aumento-un-150-durante-el-aislamiento/
- ✓ Aznar, R. (2015, 25 agosto). *LA CIBERSEGURIDAD A UN CLIC DE TU EMPRESA | PRODATOS ALCARRIA. Asesoría de Protección de Datos, LOPD, privacidad y tecnologías de la Información.* PRODATOS ALCARRIA. Asesoría de Protección de Datos, LOPD, privacidad y tecnologías de la Información. | Asesoría de Protección de Datos, LOPD, Privacidad y Tecnologías de la Información. https://www.prodatosalcarria.es/la-ciberseguridad-a-un-clic-de-tu-empresa/

- ✓ Cámara Colombiana de Informática y Telecomunicaciones. (2019, 26 marzo). *La CCIT*. CCIT - Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/la-ccit/
- ✓ Cámara Colombiana de Informática y Telecomunicaciones. (2020, 10 diciembre). Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020. CCIT - Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/noticias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020/
- ✓ Centro de ciberseguridad industrial. (s. f.). Colombia. Recuperado 9 de octubre de 2021, de https://www.cci-es.org/maps/colombia/
- ✓ Daniels, K. (2020, 31 agosto). Ciberataques a las instituciones educativas: ¿Clases con o sin protección? Widefense. https://www.widefense.com/recursos/ciberseguridad/ciberataques-a-instituciones-educativas/
- ✓ Delitos informÃ¡ticos en Colombia. (s. f.). World Legal Corporation. Recuperado 24 de septiembre de 2021, de https://www.worldlegalcorp.com/blog/delitos-informaticos-en-colombia/
- ✓ E. (2019, 17 septiembre). Cómo gestionar los controles de acceso según ISO 27001. Escuela Europea de Excelencia. https://www.escuelaeuropeaexcelencia.com/2019/09/como-gestionar-los-controles-de-acceso-segun-iso-27001/
- ✓ Editorial La República S.A.S. (2021, 2 junio). ¿Qué castigos estipula el Código Penal para los delitos informáticos como la estafa?

https://www.asuntoslegales.com.co/actualidad/que-castigos-estipula-el-codigo-penal-para-los-delitos-informaticos-como-la-estafa-3180022

- ✓ Editorial La República S.A.S. (2021a, febrero 16). Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. 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
- ✓ Estudio de ciberseguridad en el Sector Público. (2019, 5 marzo). Deloitte Colombia. https://www2.deloitte.com/co/es/pages/risk/articles/el-estudio-de-ciberseguridad.html
- ✓ G. (2020, 22 enero). ¿Cuáles son delitos informáticos más comunes? - Escuela Derecho. Escuela de Ciencias Jurídicas. https://escuelacienciasjuridicas.com/delitos-informaticos-mas-comunes/
- ✓ Gonzalez, F., Equipo Editorial Py+, & Equipo Editorial Py+. (s. f.). ¿Por qué es importante la ciberseguridad en las pymes? Pymas. Recuperado 11 de octubre de 2021, de https://www.pymas.com.co/ideas-para-crecer/ayuda-legal/ciberseguridad-pymes-colombia
- ✓ Grupo Investigativo de Delitos Informáticos - GRIDI. (2009). L Investigación tecnológica de los Delitos Informáticos. Bogotá.
- ✓ INFRAESTRUCTURA DE EDUCACIÓN VIRTUAL: DESAFÍOS EN CIBERSEGURIDAD – Latin Pyme. (s. f.). INFRAESTRUCTURA DE EDUCACIÓN VIRTUAL. Recuperado 11 de octubre de 2021, de https://www.latinpymes.com/infraestructura-de-educacion-virtual-desafios-en-ciberseguridad/
- ✓ Instituto Nacional De Ciberseguridad. (2020, 5 marzo). Herramientas de ciberseguridad. INCIBE. https://www.incibe.es/protege-tu-empresa/herramientas.

- ✓ Los ciber-riesgos en el sector Manufacturing. (2017, 2 marzo). Deloitte Spain. https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciber-riesgos-manufacturing.html
- ✓ Mx, D. (2018, 18 junio). El sector educativo también sufre los efectos de la ciberseguridad. Destino Negocio. https://destinonegocio.com/mx/gestion-mx/sector-educativo-tambien-sufre-los-efectos-de-la-ciberseguridad/
- ✓ P. (2020, 10 diciembre). *Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020*. Portafolio.co. https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412
- ✓ P. (2021, 7 octubre). Davivienda se pronuncia sobre casos de fraude y ciberseguridad. Portafolio.co. https://www.portafolio.co/negocios/empresas/davivienda-se-pronuncia-sobre-casos-de-jessica-de-la-pena-y-carlos-sarria-en-fraude-y-ciberseguridad-557117
- ✓ Policia Nacional de Colombia. (s. f.). Centro Cibernético Policial. Centro Cibernético Policial. Recuperado 9 de octubre de 2021, de https://caivirtual.policia.gov.co/
- ✓ Policía Nacional de Colombia. (2020, 1 julio). Normatividad sobre delitos informáticos. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
- ✓ Uid, D. L. D. C. I. D. U.-. (s. f.). Los Tipos De Delitos Informáticos Más Comunes En Colombia | Uid - Unidad de Investigación Criminal de la Defensa. Delitos informáticos comunes. Recuperado 24 de septiembre de 2021, de https://uid.org.co/los-tipos-de-delitos-informaticos-mas-comunes-en-colombia/
- ✓ T. (s. f.). Las principales modalidades de ciberdelitos y cómo protegerse. El Tiempo. Recuperado 12 de octubre de 2021, de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberdelitos-en-colombia-cuales-son-las-principales-modalidades-

568454#:%7E:text=Colombia%20no%20est%C3%A1%20exenta%20de,ciento%20frente%20al%20a%C3%B1o%20anterior.

- ✓ You are being redirected. . . (s. f.). Infolaft. Recuperado 12 de octubre de 2021, de https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/