La ciberseguridad política clave dentro de las organizaciones

Universidad Santo Tomás Tunja.

Facultad de Contaduría

Especialización en Auditoría y Aseguramiento de la Información

Docente: coronel (r) Fredy Bautista García

Estudiantes:

David Leonardo González Diaz - Saul Sebastián Pulido Sainea

Tunja - Boyacá

2021

TÍTULO: LA CIBERSEGURIDAD POLÍTICA CLAVE DENTRO DE LAS ORGANIZACIONES

Autores: David Leonardo González – Saul Sebastián Pulido Sainea

Resumen: El presente artículo nos da una noción del problema de vulnerabilidad que tienen actualmente muchas entidades y organizaciones en Colombia por el desconocimiento en ciberseguridad por parte de los sus funcionarios y debilidades en el control interno sobre el mencionado tema, la ausencia de políticas y de manuales de ciberseguridad sumado a los bajos controles que muchas veces tienen las entidades en este tema han creado una oportunidad para que los ciberdelincuentes pongas sus ojos en las empresas, organizaciones y emprendimientos, para enfrentar dicho problema se realiza una investigación se revisan diferentes autores y se crean algunas soluciones prácticas que podrían ser adoptadas por las entidades con el fin de disminuir su vulnerabilidad y caer bajo algún ciberataque.

Palabra Claves: Pymes, Ciberseguridad, Ciberataques, Control Interno, Capacitación, Ransomware, Ataques BEC.

Abstract: This article gives us a notion of the vulnerability problem that SMEs in Colombia have due to the lack of knowledge about cybersecurity on the part of their officials and weaknesses in internal control on the aforementioned issue, the absence of cybersecurity policies and manuals, added to The low controls that entities often have on this issue have created an opportunity for cybercriminals to put their eyes on SMEs. To face this problem, an investigation is carried out, different authors are reviewed and some practical solutions are created that could be adopted by entities in order to reduce their vulnerability if they fall under a cyberattack.

Keywords: SMEs, Cybersecurity, Cyberattacks, Internal Control, Training, Ransomware, BEC attacks.

Introducción: En este artículo se tiene un objetivo general, el cual dará una solución práctica al problema planteado, del objetivo general se desprenden 4 objetivos específicos que se mencionan en la página 3 de este artículo. Nos enfocamos en dar a conocer la problemática que está latente y es un riesgo en todo momento y tratamos de generar conciencia con cifras que aportan algunos autores en el país, se pretende desde este artículo que el control interno de las entidades asuma este problema como real y que sea de gran importancia para ellos.

El control interno juega un papel crucial para empezar a dar solución o ejercer un control estricto sobre esta problemática, si se empiezan a adoptar los controles necesarios en cada organización disminuirá la vulnerabilidad de la entidad frente a este problema. Por ende, el Control interno debe ser un proceso que se tiene que ir evaluando y verificando a menudo si genera el impacto necesario en los funcionarios de la organización.

Por lo anterior, El área de control interno tiene que estar en constante aprendizaje sobre las nuevas modalidades y formas que tienen los cibercriminales para realizar ataques a las entidades, su constante retroalimentación de nuevas prácticas será fundamental para su organización y realizar capacitaciones a su personal y crear nuevas políticas de ciberseguridad, para mantener en bajos niveles la vulnerabilidad de su entidad.

OBJETIVO GENERAL:

Dar a conocer el creciente problema de ataques cibernéticos que sufren las organizaciones en Colombia, y la necesidad de sensibilización al interior de las mismas.

OBJETIVOS ESPECÍFICOS:

1. Presentar los tipos de ataques más utilizados por los ciberdelincuentes en Colombia.

2. Ofrecer opciones a las entidades y organizaciones para establecer una cultura en ciberseguridad.

3. Fortalecer el control interno mediante la entrega de un instrumento escrito que sirva de consulta y guía para la definición de necesidad de asignación de nuevos roles con personal experto en gestión de políticas organizacionales de prevención y mitigación de amenazas cibernéticas.

4. Generar escenarios de concienciación y sensibilización en las organizaciones mediante información actualizada de nuevas tendencias de ciberataques y amenazas.

MARCO TEÓRICO

Es importante empezar definiendo el control interno en las organizaciones; pues según Juan R. Conde-Camilo profesor de la universidad de la Habana Cuba, es un sistema para el perfeccionamiento, mejora y gestión empresarial que busca un impacto positivo y de crecimiento en los gobiernos corporativos organizacionales siendo este una herramienta para controlar y mitigar los riesgos que se puedan presentar en la actividad empresarial diaria.

En los últimos tiempos mediante la globalización y crecimiento tecnológico mundial los cambios que ha sufrido el ámbito empresarial son notorios a la hora de analizar sus procesos misionales y comerciales ya que las empresas han adaptado nuevos procesos tecnológicos estratégicos para desarrollar de manera eficiente sus objetivos organizacionales.

Con este avance tecnológico empresarial también surgieron amenazas como el auge de los ciber-crímenes y sus técnicas para el robo y secuestro de activos e información valiosa de la empresa mediante softwares malignos y estrategias de engaño con el fin de afectar la seguridad cibernética de las empresas.

La Asociación Colombiana de Ingenieros de Sistemas ACIS ratifica que hasta hace muy poco los riesgos cibernéticos eran incipientes y de grado bajo-medio pero con el impacto sufrido por la penetración de las TICS y su importancia empresarial, siendo la información el activo más valioso de muchas organizaciones; se elevó la responsabilidad del control interno de las empresas frente a la seguridad cibernética para prevenir y mitigar, además de crear planes de contingencia para afrontar amenazas y ciberataques a los sistemas y software de información de la organización.

La necesidad de darle solución al problema de los ciberataques surge del gran auge que han tenido estos mismos en los últimos años ya que se registra un aumento en las denuncias físicas y virtuales, el cual se registra en la siguientes estadísticas: año 2015 - 7.523 denuncias, año 2016 - 11.225 denuncias, año 2017 - 15.840 denuncias, año 2018 - 22.524 denuncias, año 2019 – 17.531 denuncias, los porcentajes de estas denuncias se reparten de la siguiente manera 54.5% fueron denuncias físicas y el 45.5% fueron denuncias virtuales (TicTac, 2019), los ciberdelincuentes no solo se enfocan en tratar de robar a las personas naturales, sino que sus ojos están puestos en las pymes, ya que muchas de las entidades no cuentan con un robusto sistema de seguridad o no tienen unas buenas políticas de ciberseguridad, sumado a esto muchos de los funcionarios no tienen bases sólidas sobre ciberseguridad.

> La ciberseguridad es un tema de moda y se puede convertir en un problema para las organizaciones ya que muchas no cuentan con el personal preparado para abordar este tema y realizar aportes a la entidad. El autor Castillo, A., Bruzza, M., & Tupia, M. (2021). Estado del arte sobre la identificación de amenazas no intencionales de ciberseguridad de parte de personal interno en instituciones públicas. Por su parte la Revista Ibérica de Sistemas e Tecnologías de Informação, (E41), 70-82. página 3, nos da una definición sobre ciberseguridad tomada y adaptada de la ISACA, “Según ISACA, define la ciberseguridad como la disciplina que permite la “protección de activos de información digitales, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (ISACA, 2015)”.
>
> Los ciberdelincuentes teniendo en cuenta que muchas entidades no están preparadas para manejar estos temas, están aprovechando la brecha de conocimiento en la materia para realizar ataques a las entidades en el país, un estudio realizado por los autores Adriana Ceballos López, CR(RA) Fredy Bautista García, Lorena Mesa Guzmán, Carlos Argaez Quintero nos muestra que “La dinámica actual del Cibercrimen en Colombia refleja un crecimiento gradual en el

> número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad, A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019”,página 7
>
> “El delito informático más denunciado en Colombia es el Hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca”, libro página 7
>
> Los ataques cibernéticos se identifican de distintas formas, “Los incidentes más reportados en Colombia siguen siendo los casos de Phishing con un 42%, la Suplantación de Identidad 28%, el envío de malware 14% y los fraudes en medios de pago en línea con 16%.” Libro pág. 7, este tipo de ataques se han detectado en varias entidades, y aún no se le da la importancia a un problema que nos puede afectar a todos por igual.

El estudio realizado por la Universidad de Córdoba en el presente año sobre delitos cibernéticos y su respectivo impacto tanto en la economía común como en el comercio electrónico en Colombia, habla sobre el alto riesgo de que las empresas PYMES sean afectadas por las amenazas y ataques cibernéticos en el desarrollo de sus operaciones misionales; ya que estas cuentan con un buen desarrollo, fortalecimiento y crecimiento organizacional considerable en cuanto a su seguridad y educación cibernética para prevenir, mitigar amenazas y ataques en las empresas colombianas.

La educación y seguridad cibernética (informática) es uno de los pilares fundamentales que posee el sector educativo en este último tiempo, señala la universidad piloto de Colombia según estudios realizados mediante observación, encuestas y entrevistas a docentes, estudiantes y profesionales en diversos ámbitos laborales y estudiantiles que la importancia es alta a la hora de hablar sobre la capacitación y formación de profesionales capaces de asegurar y proteger información, datos y documentos además de detectar y afrontar amenazas y ataques cibernéticos en la organización en su actividad diaria profesional y crecimiento integral según la mega tendencia y crecimiento global informático en el mercado.

Los sistemas de información se han convertido en herramientas estratégicas de crecimiento y competitividad para las empresas ya que estos son de gran ayuda para la mejora continua y el cumplimiento de metas organizacionales y misionales a la hora de prevenir, mitigar y resolver problemas tanto de comunicación y control interno, como de aseguramiento de la información y seguridad cibernética según un artículo realizado por la revista universidad y sociedad.

Es muy común encontrar en las organizaciones redes de WI-FI las cuales no cuentan con protocolos de seguridad lo suficientemente robustos para repeler ataques externos y proteger la información que se comparte a través de esta red, actualmente existen

varios protocolos de seguridad para ayudar a proteger las redes, algunos son de alto costo pero garantizan una baja vulnerabilidad de la red, uno de ellos es el protocolo WPA3 (WI-FI Protected Access) en su versión 3, este es un protocolo que se utiliza con el fin de proteger las redes inalámbricas.

Tabla Número 1.

Ataques cibernéticos más utilizados en Colombia

Ataque BEC	(Business Email Compromise), este ataque consiste en secuestrar las cuentas empresariales, el cibercriminal trata de suplantar funcionarios de gran rango en las entidades para realizar acciones no autorizadas y defraudar la entidad, se pueden realizar envíos a proveedores en tiempos no autorizados o mercancía que no llega a su destino para ser posteriormente hurtada
RANSOMWARE	Secuestro de datos, es uno de los ataques más subestimados en Colombia, el operar del ciberdelincuente es el envío masivo de correos electrónicos, con asuntos susceptibles de entidades gubernamentales o alertas de robo de información que llaman la atención de la víctima, utilizan esto como fachada para llevar a la víctima a enlaces maliciosos.
Ataque DDOS	El ataque DDOS, consiste en deshabilitar algún sistema, un servidor o una aplicación, impide su normal funcionamiento.
MALWARE	El Malware es un software malicioso que trata de ser instalado en los ordenadores, celulares o tabletas sin consentimiento del usuario, tratando de acceder por medio de este a información valiosa de la víctima.
PHISHING	El Phishing es un engaño basado en la ingeniería social, tiene como propósito engañar a la víctima, haciéndose pasar por una empresa o por una persona, con el fin de que la víctima revele información como contraseñas de correos, códigos de seguridad de sus entidades bancarias, por lo general se utilizan correos electrónicos mensajes de texto o mensajes directos en las redes sociales para realizar dicho engaño.

Nota: Esta tabla muestra el significado de los ataques más utilizados en el país.

Muchas entidades y organizaciones en el país son víctimas de estos ataques, y en ocasiones los ciberdelincuentes no solo se enfocan en tratar de robar data de las entidades, ellos también van en busca de la información personal de los funcionarios, si no logran realizar un ataque a la entidad buscan realizar un ataque personalizado.

Una técnica utilizada por los delincuentes es el vishing, este tipo de ataque consiste en realizar una llamada a sus víctimas por teléfono haciéndose pasar por otra persona de esta manera generar una confianza en la víctima, y convencerla para que revele información personal como lo son contraseñas nombres de usuario, pin de transacciones electrónicas o información confidencial de la entidad donde labora.

Los funcionarios en las entidades pueden asumir el rol de firewall humano y llegar a ser la primera línea de defensa contra las técnicas de ataques que utilizan los ciberdelincuentes, esto se logra a través de capacitaciones al personal por parte de expertos en el tema.

Una buena práctica para las organizaciones es la de tener en cuenta los siguientes 10 elementos que pueden ayudar a protegerlas de alguna técnica de ataque por parte de un ciberdelincuente.

1. Respuesta ante incidentes.
2. Contraseñas.
3. Protocolo de red (WPA).
4. Navegación segura y firewall humano.
5. Ingeniería Social y suplantación de identidad.
6. Privacidad
7. Seguridad física.
8. Movilidad y información en la nube.
9. Copias de seguridad.
10. Políticas de ciberseguridad.

El estado del Arte:

Ejemplos de autores que dieron solución a un tema similar al nuestro.

1. Modelo de identificación de ciber amenazas para PYMES de servicios tecnológicos usando herramientas de Data Analytics.

- Este proyecto tiene como propósito mejorar la capacidad que tienen las empresas pequeñas y medianas de detectar Ciber amenazas que puedan encontrarse en sus ambientes, y que no hayan sido detectadas por las herramientas de seguridad tradicionales, como los antivirus. (Chancafe-Gutierrez, 2020)

2. El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia; Delitos cibernéticos. En el presente estudio monográfico se abordará el impacto del delito cibernético en las operaciones de comercio electrónico en Colombia, así mismo los riesgos que incurren al momento de hacer operaciones

de compra o venta, transacciones en línea, etc. Además de ello se conocerá el crecimiento que ha tenido Colombia durante los últimos años en cuanto a operaciones de comercio electrónico, los diferentes sectores en los que ha crecido considerablemente y el comportamiento que ha tenido con la actual situación de pandemia Covid-19. (Peralta-M.L-Ibarra, 2021)

3. Estado del arte sobre la identificación de amenazas de ciberseguridad en el control interno en instituciones públicas y privadas. (Bruzza&Tupia, 2021)
4. La dinámica actual del cibercrimen en Colombia, estudio sobre el desconocimiento de ataques cibernéticos. (Bautista-Mesa&Quintero, 2015)

Presunción de Solución:

Nombre de la Solución: Campaña Empresarial de educación para la prevención, mitigación y resolución de amenazas y ataques cibernéticos.

Teniendo en cuenta que “el 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante (TicTac, 2019), la problemática radica en el desconocimiento de las técnicas que utilizan los cibercriminales para realizar los ataques, que varían desde darle un clic a una publicidad de origen desconocido, abrir un correo electrónico que contiene información engañosa y no logremos identificar, hasta entrar a un sitio no debido a través de un navegador de internet.

Lo anterior demuestra que los factores en torno a los ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías”.

A partir de lo anterior resulta claro que las Pymes tendrán que implementar un modelo de políticas de seguridad informática que se ejecute efectivamente cuando se presenten ciber amenazas dando solución y aviso de alerta a los funcionarios previniendo caer en esta amenaza; este modelo debe ser desarrollado y gestionado por un experto en ciberseguridad para redactar las políticas se seguridad.

Igualmente es necesario realizar una adecuada capacitación en seguridad informática a cada uno de los funcionarios de la entidad, generando conciencia en el trabajador sobre ciberseguridad, informando las amenazas latentes a las que se está expuesto en todo momento y una posible probabilidad de ser víctima de un ataque.

FORTALECIMIENTO CONTROL INTERNO:

Con el ánimo de brindar asesoría para el fortalecimiento de políticas organizacionales de prevención y mitigación de amenazas cibernéticas; es importante que las organizaciones consideren un nuevo rol dentro de la organizaciones que asuma las funciones de control interno en asuntos de Ciberseguridad, este perfil profesional idóneo para el cargo de líder

especialista gestión del departamento de control interno en el énfasis en ciberseguridad y tecnologías de la información, tendré en otras las siguientes responsabilidades:

Implementar y mantener una política de seguridad integral mediante estrategias que buscan el objetivo de resguardar toda la información de la compañía. Con actividades laborales como:

Desarrollar e implementar las políticas y procedimientos de seguridad. Monitorear su cumplimiento.
Disuadir, Detectar y Responder a incidentes de seguridad física.
Realizar actividades de gestión de riesgos (planificación, detección, mitigaciones).
Gestionar incidentes y riesgos para garantizar la continuidad del negocio, protegiendo los activos críticos.

Debe tener competencias como la capacidad para evaluar los riesgos y basados en los mismos.

Diseñar, ejecutar políticas y mantenerlas.
Implementar medidas, sistemas de información y seguridad informática en la organización.
Además, es muy importante que disponga de pensamiento analítico, iniciativa y capacidad de resolución de problemas.
Capacidad organizativa, ateniéndose a un orden propio que le facilite el acceso a lo que pueda necesitar, así como intereses en medir el desempeño de los procesos.
Capacidad de trabajar en equipo, con buen manejo de las relaciones interpersonales estando dispuesto a compartir información y conocimientos y a tomar en cuenta a los usuarios.
Orientación a la mejora continua con capacidad para influenciar a la organización.

.

ESTUDIOS: Ingeniero de sistemas o licenciado en sistemas con especialización en ciberseguridad aplicada a sistemas de información.

MISIÓN DE LA OCUPACIÓN: Proveer un marco de metodología y estandarización de seguridad de información a la organización y sus proyectos, detectando en forma temprana causas de desvíos, implementando y administrando sistemas, políticas y normatividad de seguridad informática. CESSI.ORG. (n.d.). https://www.cessi.org.ar/perfilesit/detalle-de-especialista-en-seguridad-de-la-informacion-14

POLÍTICAS DE CIBERSEGURIDAD

Ahora bien, desde el diseño de la política de Ciberseguridad, a continuación, se identifican los elementos a considerar dentro de la construcción de la misma, así:

1. La organización se encargará de dar a conocer a sus funcionarios de todos los niveles organizacionales, las técnicas utilizadas por los ciberdelincuentes, para robar información, suplantar personas o instalar softwares maliciosos que puedan atentar con el desarrollo normal de los procesos de la organización, de esta forma se puede fomentar una cultura de ciberseguridad en cada uno de los funcionarios de la entidad.

2. Dentro de la organización se debe contar con un departamento o una dirección de informática, el cual cuente con personal calificado en ciberseguridad y pueda atender cualquier irregularidad que se presente y brindar apoyo inmediato a cualquier funcionario sin importar su nivel organizacional.

3. Se debe contar con credenciales de acceso para los funcionarios, para acceder a las redes o software que involucren procesos de cada una de las dependencias, será responsabilidad de la dirección de informática crear los usuarios de cada funcionario y guiar a los funcionarios en la creación de sus contraseñas, las contraseñas deben tener mínimo 8 caracteres y deben incluir una mayúscula y un número.

4. Las contraseñas que utilizan los funcionarios deben ser cambiadas con periodicidad no mayor a 3 meses, esto con el fin de disminuir la vulnerabilidad de la organización.

5. Es responsabilidad de cualquier funcionario de la entidad sin importar su nivel organizacional la ciberseguridad, esto a través del buen uso y buenas prácticas en las acciones relacionadas con la manipulación de dispositivos electrónicos conectados a cualquier red que pertenezca a la organización, se debe fomentar una cultura de buena navegación que sea una navegación en internet a través de navegadores seguros evitar ejecutar ventanas emergentes y prestar mucha atención a los correos que llegan a las respectivas bandejas de entrada tomarse el tiempo necesario para analizarlos y evitar dar clic innecesarios en URLS o hipervínculos que se desconozca su procedencia.

6. Se deben realizar actualizaciones e instalaciones de software nuevos por parte de funcionarios del departamento o dirección de informática.

7. Para protección de la información es necesario realizar periódicamente copias de seguridad de la información valiosa de cada dependencia de la organización.

8. Contar con un protocolo de ciberseguridad, con el cual se pueda tener una respuesta en el menor tiempo posible si se está ante cualquier ciberataque y proceder a realizar las acciones necesarias para repeler dicho ataque, es necesario que las organizaciones ajusten sus protocolos de ciberseguridad teniendo en cuenta el tamaño

de la entidad, el número de funcionarios que laboran, las áreas o departamentos en las que se divide la organización y las herramientas informáticas, se recomienda que el protocolo cuente con un inventario por áreas o departamentos de los dispositivos electrónicos, sistemas y las aplicaciones, esto con el fin de identificar cada una de las posibles fuentes de vulnerabilidad.

Es importante que estas políticas de Ciberseguridad sean divulgadas, estudiadas y explicadas por parte del personal idóneo de la organización, al resto de funcionarios de la organización sin importar su nivel organizacional, con estas políticas de ciberseguridad y dando cumplimiento a cada una de ellas podemos ayudar a fortalecer la seguridad de la organización.

Las políticas se pueden actualizar o cambiar dependiendo de las necesidades de cada organización, está en manos de los expertos del departamento de informática, ellos se encargarán de evaluar la vulnerabilidad actual de la entidad y adaptar las nuevas políticas para proteger la organización.

Como un complemento de las políticas de seguridad, las organizaciones deben invertir en software y equipos que puedan ayudar a proteger sus dispositivos y cada una de las redes que se creen y se utilicen dentro de la organización, es importante que se actualicen y se renueven los equipos que se utilizan.

METODOLOGÍA

A continuación, se describen las soluciones estratégicas que contribuyen a la sensibilización en materia de ciberseguridad y la disminución del problema de analfabetismo cibernético:

A través de un video didáctico de sensibilización se expondrán los temas más importantes en cuanto a la ciberseguridad y las amenazas cibernéticas; así como la realización de un modelo de manual explicando los procedimientos a seguir por las organizaciones cuando se encuentren bajo un ataque cibernético.

Por medio de una guía en forma de cartilla los funcionarios desarrollarán un taller evaluando la información brindada en el video llevando la teoría a la práctica con el desarrollo de un ejemplo de caso empresarial de ciberataque.

Mediante la gestión de vacantes para profesionales especialistas en aseguramiento de la información y ciberseguridad; además de pruebas de ascenso según conocimiento y experiencia para funcionarios de la entidad evaluando su escepticismo profesional ante la ciberseguridad.

Conclusiones

- Por medio de este artículo se plantearon actividades y procesos para la mitigación y resolución práctica al desconocimiento que tienen algunas empresas PYMES sobre el tema de ciberseguridad. Comprendiendo que en el mercado empresarial las mega tendencias de expansión, crecimiento corporativo y mejora continua se lleva a cabo a través del e-commerce (comercio electrónico) haciendo de este tema un pilar fundamental, una cultura organizacional y estrategia de educación para el fortalecimiento en ciber seguridad para las empresas.
- Todas las entidades de Colombia que tengan acceso al artículo pueden generar una cultura de autoprotección ya que mediante su desarrollo se buscó disminuir al máximo los niveles de vulnerabilidad en caso de un ciberataque mediante la culturización y educación en el tema. También se brinda un conocimiento al área de control interno de las entidades y que, a partir de este nuevo conocimiento adquirido, se realicen nuevas políticas de ciberseguridad para la organización.
- Se hace énfasis en la contratación del personal idóneo y experto en temas de Aseguramiento de información y ciberseguridad, para que apoyen la redacción de las políticas nuevas de ciberseguridad y capaciten el personal, recomendando que todas las entidades deberían crear un manual de procedimientos preventivos y de acción frente a la materialización de estar bajo un ataque cibernético y que cada funcionario pueda proceder de manera adecuada.
- Se desarrolló el articulo y se da su relevancia basándose en datos históricos y situaciones socio-empresariales en donde se analizó la importancia de este tema para las empresas y el impacto negativo que este fenómeno de los ciberataques trae paras las organizaciones, además de evaluar las pérdidas de propiedad intelectual, económicas que dejan este fenómeno en las empresas.

Referencias

Bautista-Mesa&Quintero. (2015). *www.ccit.org.* Obtenido de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Bruzza&Tupia. (2021). *Revista Ibérica de Sistemas e Tecnología de Información.* Obtenido de https://search.proquest.com/openview/4fc3316c510c3b225e5378667120e7e6/1?pq-origsite=gscholar&cbl=1006393

Chancafe-Gutierrez. (2020). *UPC.EDU.* Obtenido de https://repositorioacademico.upc.edu.pe/handle/10757/653631

Peralta-M.L-Ibarra. (2021). *Universidad de Córdoba-Colombia.* Obtenido de https://repositorio.unicordoba.edu.co/handle/ucordoba/3949

Ciberseguridad y Ciberdefensa en Colombia Rubén Darío Laverde Castillo1, Miguel Hernández Bejarano
https://fundacionavenir.net/revista/index.php/avenir/article/view/106/60

La importancia del componente educativo en toda estrategia de Ciberseguridad
https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/9

Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad
http://www.imjst.org/wp-content/uploads/2019/02/IMJSTP29120135.pdf

Auditorías en ciberseguridad: un modelo de aplicación general para empresas y naciones
http://openaccess.uoc.edu/webapps/o2/handle/10609/124326

El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia
https://repositorio.unicordoba.edu.co/handle/ucordoba/3949

Diseño de un sistema de gestión de seguridad de la información para el área de talento humano de la secretaria de educación de Fusagasugá basado en la norma NTC-IEC ISO 27001:2013
http://repository.unipiloto.edu.co/handle/20.500.12277/9854

HERRAMIENTA DE SEGURIDAD PARA LOS ACTORES DE LA CADENA DE SUMINISTROS – DIJIN
https://www.policia.gov.co/sites/default/files/descargables/herramienta_de_seguridad_digital1.pdf

Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación
https://cybertesis.unmsm.edu.pe/handle/20.500.12672/16013

Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación
https://hdl.handle.net/20.500.12672/16013

Implementación de programas de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano
http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/18475

Incidencia del factor humano en la seguridad de la información de las organizaciones públicas de categoría 6.
https://repository.unad.edu.co/handle/10596/38893

Desafíos nacionales frente a la ciberseguridad en el escenario global un análisis para Colombia
https://dialnet.unirioja.es/servlet/articulo?codigo=7667839

El Sistema de Control Interno para el Perfeccionamiento de la Gestión Empresarial en Cuba (Sistema de Control Interno para la Mejora del Gobierno Corporativo en Cuba)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2396834