RIESGOS Y VULNERABILIDADES ASOCIADOS AL FACTOR HUMANO COMO EL ESLABÓN MÁS DÉBIL Y EL PAPEL DE LA CIBER CONCIENCIA COMO ELEMENTO ESTRATÉGICO PARA MINIMIZAR EL IMPACTO DE LOS CIBERATAQUES EN LAS ORGANIZACIONES PÚBLICAS Y PRIVADAS DE COLOMBIA

JORGE IVAN GAVIRIA RESTREPO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2022

RIESGOS Y VULNERABILIDADES ASOCIADOS AL FACTOR HUMANO COMO EL ESLABÓN MÁS DÉBIL Y EL PAPEL DE LA CIBER CONCIENCIA COMO ELEMENTO ESTRATÉGICO PARA MINIMIZAR EL IMPACTO DE LOS CIBERATAQUES EN LAS ORGANIZACIONES PÚBLICAS Y PRIVADAS DE COLOMBIA

JORGE IVAN GAVIRIA RESTREPO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Nombre
Joel Carrol Vargas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

GLOSARIO

Ciber: Prefijo del adjetivo cibernético, forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual: ciberespacio, cibernauta, etc.

Ciber espacio: Así se denomina al entorno artificial que se desarrolla mediante herramientas informáticas.

Ciber nauta: Persona que utiliza servicios informáticos del ciberespacio.

Digital: El concepto, de todas formas, está estrechamente vinculado en la actualidad a la tecnología y la informática para hacer referencia a la representación de información de modo binario.

Hacker: Persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

IA: Corresponde a la expresión Inteligencia Artificial.

Internet: Red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

Metaverso: Es una red de entornos virtuales siempre activos en los que muchas personas pueden interactuar entre sí y con objetos digitales mientras operan representaciones virtuales, o avatares, de sí mismos.

Ordenador: Es un Sistema conformado por programas y elementos electrónicos, que en su conjunto permiten procesar y ordenar información.

OTAN: Organización del Tratado del Atlántico Norte, la OTAN o Alianza Atlántica (North Atlantic Treaty Organization, NATO en sus siglas inglesas).

Phishing: Es un método que los ciber delincuentes utilizan para engañar y conseguir que se revele información personal, como contraseñas, datos de tarjetas de crédito o de la seguridad social y números de cuentas bancarias, entre otros.

PIB: Producto Interno Bruto.

Protocolo: Conjunto de reglas que, ya sea por norma o por costumbre, se establecen para actos oficiales o solemnes, ceremonias y otros eventos. El protocolo, por tanto, son las instrucciones, o recomendaciones que se le debe dar cumplimento

Software: Es el equipamiento lógico que poseen los sistemas informáticos como computadoras y otros aparatos como teléfonos inteligentes, cajeros automáticos y diversos aparatos tecnológicos, entendiéndose por software a todos los programas, sistemas operativos y aplicaciones.

TIC: Tecnologías de la Información y las Comunicaciones. Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

Tribal: Es un adjetivo que señala a aquel o aquello perteneciente o relativo a una tribu, grupo

RESUMEN

Malware: agresión maligna con base en daño, captura, malicia, secuestro de datos, detectados en hallazgos así: email: 92%, web: 06%, otros: 01%. 2018 en EE.UU. la empresa SOFTTEK de desarrollo TIC, informó sobre agresiones con base en el ciber espacio: 88% agresiones dirigidas a trabajadores de RR.HH. con phishing, 98% agresiones con ingeniería social, 92,4% agresiones en correo electrónico. Se reveló que el 27% de agresiones se debe a personas que de alguna forma abrieron paso a la intrusión[1].

El objetivo de este trabajo es evaluar la necesidad de una conciencia en ciberseguridad que le permita a la sociedad asumir su responsabilidad frente a la protección de datos. Con este propósito se realiza la pregunta: *¿De qué manera los riesgos y vulnerabilidades de ciberseguridad asociados al factor humano y su falta de conciencia, pueden impactar negativamente las infraestructuras tecnológicas y de comunicación de las organizaciones públicas y privadas de Colombia?* Esta pregunta marca la pertinencia de un trabajo que pretende establecer concienciación en la sociedad en cuanto a ciberseguridad.

La conciencia es un marco predilecto para darle un verdadero sentido a nuestro paso y huella en el ciberespacio, por eso, se hace urgente asumir este compromiso y responsabilidad como sociedad.

[1] SOFTTEK. [Sitio web]. El 27% de ciberataques están ocasionados por empleados. [Consulta: 18 septiembre 2021]. Disponible en: https://softtek.eu/tech-magazine/cybersecurity/el-27-de-los-ciberataques-estan-ocasionados-por-el-personal-de-la-empresa/

INTRODUCCIÓN

Los ciber ataques se han convertido en el pan de cada día y absolutamente ninguna empresa debe sentirse exceptuada de tal riesgo, por eso se hace importante involucrar la necesidad de una ciber conciencia en las empresas públicas y privadas de Colombia

Ni la falta de conciencia en el ciberespacio, ni su presencia en las empresas públicas y privadas de Colombia están lejos de consecuencias, negativas unas y positivas otras, todo depende de la respuesta empresarial colombiana. Su ausencia, es un riesgo inminente para cualquier proyecto que desee crecer y su presencia la pone en el mapa competitivo y de negocios de nuestra sociedad comercial. Gestionar el riesgo de la mano de la ciber-conciencia, es un paso decisivo para empoderarla como una herramienta eficaz, para institucionalizarla ya que permite que, tanto los procesos internos sean al detalle, como los procesos de intercambio comercial, sean más seguros y menos expuestos a los ciber ataques.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

- ***SOFTTEK,*** es una empresa suministradora mundial orientada a desarrollo TIC que realizó un informe analítico basado en una fuente como lo es Verizon que es una empresa de telefonía de EE. UU. y del cual se concluye que las agresiones tienen como base el ciberespacio en el 2018[2]:
    - 88% de agresiones se dirigieron a trabajadores de RRHH dentro de una base social en la búsqueda de conocimiento por medio de información personal.
    - 98% en contexto económico se le asigna a ingeniería social.
    - 93% de agresiones, un 92,4% se les asignan a ganchos puestos en correo electrónico para que la victima de clic y consecutivamente ser infectado.
    - El malware obedece a una agresión maligna que se involucra como software con base en daño, captura, malicia, secuestro de datos detectado así:
        - Email: 92%
        - Web: 6%
        - Otros: 1%
    - 27% de agresiones se debe a personas que tienen trato o que trabajan con la organización en alguna de sus formas.
        - Un 2% son asociados y/o empleados en la antigüedad
        - Un 2% son nuevos asociados
- ***DELOITTE***, marca con la cual se agrupa un personal profesional en 150 países y prestando servicios de auditoría, consultoría, gestión del riesgo, impuestos, juristas.

  DELOITTE analizó profusamente ciber ataques cuya característica era el ramsomware y determinó que detrás de este suceso hubo personal que por descuido o desconocimiento permitieron este impase:

[2] SOFTTEK. [Sitio web]. El 27% de ciberataques están ocasionados por empleados. (Consulta: 15 de octubre 2021). Disponible en: https://softtek.eu/tech-magazine/cybersecurity/el-27-de-los-ciberataques-estan-ocasionados-por-el-personal-de-la-empresa/

- Con *la base social del phishing* involucrando el correo electrónico o un enlace y por medio del cual se busca infectar, dañar, secuestrar.
- En *la web* por medio de sitios comprometidos previamente y al cual no se tuvo las prevenciones pertinentes.
- *Buscando la contraseña privada a la fuerza o en forma bruta.*

➢ Como resultado: sucedió 12 y 16 de mayo de 2017

- Se empleó WannaCry que es un gusano informático que encripta el archivo personal o corporativo secuestrándolo. 180 países y 360.000 ordenadores comprometidos en un ataque masivo.
- Según otras fuentes dice DELOITTE, hubo 15.000.000 de infecciones con sus respectivas replicas[3].
- El gusano llegó a nueve mil quinientos distribuidores de conexión a internet.

Los resultados económicos globales fueron determinantes, golpeando a muchas empresas profundamente ya que esa es la razón de los ataques, establecer un cobro y por otro la respuesta técnica empresarial que genera otro costo, pero estos resultados económicos que, aunque revisten mucha importancia, no son objeto de este estudio.

- ***EFE***, es una agencia de noticias internacional que sirve de fuente a prensa y televisión, radiodifusoras y en el ciberespacio, mundialmente conocida y respetada por su seriedad y nivel de competencia.

Produce un informe muy actualizado a 2021[4]:

- Comparado a los primeros ocho meses del año dos mil veinte a hoy, las agresiones aumentaron en un veinte cuatro por ciento.
- Con base en un informe de Kaspersky, así:

  - Ecuador 75%
  - Perú 71%
  - Panamá 60%
  - Guatemala 43%
  - Venezuela 29%

[3] DELOITTE. [Sitio web]. ¿Qué impacto ha tenido el ciber incidente de WannaCry en nuestra economía? [Consulta: 17 de octubre 2021]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Informe-WannaCry.pdf

[4] EFE. [Sitio web]. Los ciberataques en Latinoamérica han aumentado un 24 % este año. [Consulta: 11 de octubre 2021]. Disponible en: https://www.efe.com/efe/america/tecnologia/los-ciberataques-en-latinoamerica-han-aumentado-un-24-este-ano/20000036-4619548

- *El informe revela*, que ***son los cibernautas quienes abren el acceso a esta clase de intrusión***. El panorama en centro y América latina con el malware como principal amenaza cada treinta y cinco segundos:

    - Brasil 1390 intenciones x minuto
    - México 299 intenciones x minuto
    - Perú 96 intenciones x min
    - Colombia 87 intenciones x minuto
    - Costa Rica, Guatemala, Panamá, fueron atacados en febrero y junio, según el CEO de Kaspersky hay un propósito especial de los ciberdelincuentes en estos tres países que no se logra descubrir.

- La modalidad para establecer la comunicación maliciosa con personas quienes dan entrada a los ataques es por medio de:

    - Archivos PDF y troyanos que buscan con especialidad tarjetas de crédito.
    - Phishing social que busca los correos y al cual mandan información publicitaria malintencionada.
    - El especialista Fabio Assolini dice, el ataque “la mano fantasma” incita a personas a dar clic y descargar información que contiene un software que vigila y aun estando apagado el dispositivo, se manipula remotamente.

De lo anterior se concluye que la incidencia del cibercrimen es una tendencia siempre creciente, incidencia que no siempre esta ajustada a una respuesta técnica y moderna con base en estándares o cripto-respuestas. El cibercriminal sabe muy bien que las empresas están también conformadas por personas y que estas son una base vulnerable que para ellos es la puerta por donde pueden entrar en conexión con los activos corporativos.

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera los riesgos y vulnerabilidades de ciberseguridad asociados al factor humano y su falta de conciencia, pueden impactar negativamente las infraestructuras tecnológicas y de comunicación de las organizaciones públicas y privadas de Colombia?

El paradigma de la ciberseguridad que venía en progreso, por lo menos desde la oferta tecnológica para contrarrestar toda clase de ciberataques, debió replantear

sus esquemas cuando en 2019 el mundo se vio “hackeado” por la llegada de la pandemia[5].

Si antes de la pandemia las amenazas eran incisivas y recurrentes, durante la misma fue más radical y escalada, cosa que hizo más comprometido el después donde el panorama deja una sensación aún más fuerte de inseguridad. Según la revista Forbes*,* se constató que IBM había detectado el aumento de las amenazas en ciberseguridad: el 40% de empresas en Latinoamérica los impactó en forma regular, un 25% manifestó que significativamente los impactó, un 8% dijo que los ciberataques los había impactado de manera crítica[6]. Por un lado, esto evidenció la necesidad de fortalecer la ciberseguridad, ajustarse a protocolos para evitar sanciones gubernamentales por negligencia, invertir en seguros cibernéticos. Por otro lado, las empresas se vieron obligadas, por obvias razones, al teletrabajo, razón que expuso a las empresas a mayores riesgos cibernéticos.

Está claro que los ciberataques los hacen los hackers, pero realmente el malware llega a un sistema o máquina de alguna manera, sea porque el sistema contratado o comprado no respondió efectivamente o porque la puerta de entrada es *otro* objetivo criminal.

Se necesita cumplir unas características mínimas, todas las personas que tienen un dispositivo y entran al ciberespacio o que tengan un correo electrónico, podrían estar permitiendo la entrada a malware o al mismo hacker y por ende al sistema empresarial produciendo el efecto dominó.

Según se supo por intermedio de SOFTTEK, una empresa orientada al desarrollo TIC basada en una investigación de la empresa de telefonía de EE. UU., el 27% del total de intrusiones, es debido a personas emparentadas con la empresa y de alguna manera abren la puerta a los ataques:

- Respondiendo el correo electrónico con mensajes de desconocidos
- Contestando llamadas que hacen ingeniería social
- Abriendo archivos PDF que contienen troyanos
- Entrando a la web y *dando clic a todo* lo que le interesa

[5] FORD, Ealine y WECK, Winfried. [Sitio web]. Internet y pandemia en las Américas. [Consulta: 18, septiembre 2021]. Disponible en: https://www.kas.de/documents/7851262/8887001/LIBRO+INTERNET+Y+PANDEMIA+EN+LAS+AMERICAS+VF.pdf/4a2051a3-c28a-f978-1343-5a9e4168d6ee?version=1.0&t=1608242281728

[6] FORBES CENTRO AMERICA. [Sitio Web]. Forbes Staff. 2020. La ciberseguridad antes, durante y después de la pandemia. [Consulta: 11 octubre 2021]. Disponible en: https://forbescentroamerica.com/2020/07/14/la-ciberseguridad-antes-durante-y-despues-de-la-pandemia/

- No actualizando el pc, este se actualiza basado en novedades, tendencias de cibercrimen y otras para el software

Se estimó que:

- Trescientos sesenta mil ordenadores por lo menos en ciento ochenta regiones fueron atacados por la versión de malware “WannaCry”.[7]

- Según Kaspersky, Colombia registra uno punto ocho millones de intentos de ataques cibernéticos en los primeros ocho meses del presente año [2021].[8]

- Las empresas hacen lo correspondiente para dar un alto a intentos intrusivos, pero *son las personas* que abren (en un 27% del total) la entrada a la intrusión *cuando no se tienen los cuidados y la debida responsabilidad* para cumplir con los mínimos de seguridad. Se necesita una base fuerte de conciencia que permita una educación que provea más seguridad por personas en sistemas de información.[9]

[7] DELOITTE. [Sitio web]. ¿Qué impacto ha tenido el ciber incidente de WannaCry en nuestra economía? Pág 4. [Consulta: 17 octubre 2021]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Informe-WannaCry.pdf

[8] KASPERSKY. [Sitio web]. Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [Consulta: 20 septiembre 2021]. Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

[9] DELOITTE. [Sitio web]. ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía? Pág 23. [Consulta: 17 octubre 2021]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Informe-WannaCry.pdf

2 JUSTIFICACIÓN

Una empresa puede revestir todo su sistema TI de los escudos necesarios para la protección de su activo más importante como son los datos, pero el hacker consciente de ello sabe que sigue siendo vulnerable porque trabaja con humanos.

Mark Zuckerberg aparece en una foto en la prensa y el periodista llama la atención sobre su ordenador que tiene tapado el lente de la cámara de su dispositivo, imagen reveladora que solo muestra un pequeño punto de las vulnerabilidades que nos rodean, si esto lo hace un CEO como Zuckerberg consciente de la complejidad de lo que significa la privacidad, ¿porque no las empresas que trabajan sobre su modus vivendi y se mueven por intereses y competencia sobre la base de datos y/o información? Tapar el lente no es algo técnico y mucho menos sistemático, pero, nos llama a concientizarnos de la delicadeza del problema y a la vez nos deja el interrogante, ¿debe el ser humano, hacer las veces de sujeto firewall?, tal vez si o tal vez no, pero si se hace importante considerar la necesidad de establecer un nuevo paradigma que involucre tanto la conciencia como la capacidad de entendimiento para adherirse en concreto a la seguridad empresarial sin rebasar el límite de la privacidad, aunque es un cliché en cuanto esta ya está colonizada por las cookies, los permisos concedidos al instalar aplicaciones en el móvil, el rastro o huella que se deja cuando se entra al ciberespacio, en fin.

Se hace importante provocar un nuevo paradigma que involucre a la conciencia para impactar a la sociedad y su complejidad humana, pero es super necesario ayudar a disminuir al máximo el índice de intrusión y de falta de responsabilidad informática. Se ha hecho sobre las maquinas, sistemas, ciberespacio y aunque se ha involucrado a las personas, en este momento es necesario ser más agresivo en este aspecto para hacerle frente a esta situación que provoca anualmente pérdidas económicas serias a la economía de un país y aun a la del mundo.

Con este trabajo se pretende ser una voz que se levanta en el conglomerado informático para proponer que se involucre a la conciencia (como lo hace así mismo la ISO de calidad del producto 9001:2008 sobre recursos humanos en el requisito 6.2.2 sobre la toma de conciencia)[10] y gestionar un nuevo esquema, modelo o paradigma soportado sobre la infraestructura de seguridad o estándares existentes, con la salvedad de la gestión, seguimiento y control que se hará por medio de indicadores no de gestión sino de conciencia (aunque parezca abstracta no deja de ser medible) que promuevan el estricto cumplimiento para salvaguardar los activos empresariales elaborados de acuerdo al carácter y la personalidad de la empresa.

Cabe pensar o acaso decir que, si esto llega a realizarse, el mundo habrá dado un

[10] ISO. [Sitio web]. Sistemas de gestión de la calidad. [Consulta: 25 septiembre 2021]. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:9001:ed-4:v2:cor:1:v1:es

paso valioso que hará un aporte grandísimo, tanto al sector institucional y corporativo, como a la conciencia informática de quienes usan máquinas o dispositivos para hacer presencia en el mundo de los negocios.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

- Analizar los riesgos y vulnerabilidades asociados al factor humano como el eslabón más débil y el papel de la ciber conciencia como elemento estratégico para minimizar el impacto de los ciberataques, estableciendo una estrategia de seguridad basada en la ISO 27002 en las organizaciones públicas y privadas de Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Desarrollar una revisión de estado de del arte con al menos 20 referencias académicas sobre la ciberdefensa en las organizaciones.

- Desarrollar un análisis de los resultados obtenidos de la revisión del estado del arte.

- Diseñar una estrategia de ciberseguridad para las empresas públicas y privadas de Colombia basado en la ISO 27002.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El mundo está bajo el flujo permanente de la comunicación y la necesidad de conocer, de saber, de contestar muchas preguntas que aún no han podido ser contestadas y el espacio virtual llámese ciber espacio, virtualidad o internet (esta última que sin ser igual a ciber espacio, no deja de ser un sujeto análogo o variante de este) se ha convertido en un espacio predilecto para abordar todo este menú de cosas por saber. Ah todo esto, nos encontramos con todas las circunstancias que puede haber para el cibernauta o internauta y que en menor o mayor grado pueden representar un peligro al momento de entrar en el espacio virtual. Mucho se ha hablado de los cuidados que se deben tener al "navegar" en este espacio y ahora ya se habla de la concienciación que se debe tener al requerir de esta navegación en la virtualidad. Pues precisamente es mi tema, que las personas en todo el mundo y aún más en Colombia, que es el centro de mi interés, usen su conciencia, autocuidado, protección para no caer en una de tantas trampas que se pueden encontrar en el ciber espacio.

4.1.1 Antecedentes

Esta conciencia en el ciberespacio no se ha estudiado ahora, ya ha habido mucho movimiento al respecto por querer establecerla en este ambiente virtual, he aquí algunos datos al respecto.

Christof Koch, ciudadano alemán-estadounidense muy conocido por sus aportes a la neurociencia, compara el difícil entramado del cerebro formado por millones de neuronas y hace alusión a que esto nos permite la conciencia agregando que este mismo echo se parece mucho al fenómeno conocido de la internet, dejando un inquietante cuestionamiento: ¿será que la internet tendrá capacidad para pensar o albergar conciencia? *Koch*, declara que la complejidad de esta red es comparable con una estructura consciente. Pero su hipótesis va mucho más allá, el científico se atrevió a decir que la internet podría llegar a contener estados de ánimo debido a sus transistores, relación entre nodos y sin decir que tipo de estado, concluye diciendo que tendría la capacidad de sentir.[11]

Resulta que esta hipótesis tiene que ver mucho con algo que se llama **redes neuronales artificiales** más conocida como sistema conexionista que equivale al modelo computacional (busca por intermedio de una simulación por computadora

[11] RT. [sitio web]. 'Internet podría tener conciencia y gozar de sentimientos' [Consulta: 20 octubre 2021]. Disponible en: https://actualidad.rt.com/ciencias/view/52157-internet-podria-tener-conciencia-gozar-sentimientos

estudiar, analizar un comportamiento de este). Estas redes neuronales que no dejan de ser abstractas tendrían la misma capacidad del cerebro en el humano para resolver cualquier problema. Estos sistemas debido a su capacidad poseen un autoaprendizaje y de autoformación.

El campo de aplicación de estas redes neuronales estriba en establecer solución a una multiplicidad de tareas, entre ellas su aplicación para reconocer la voz, otra sería la visión realizada por computador que se efectúa para ello usando un protocolo de reglas.[12]

Todo esto estaría justificando de una u otra forma la teoría de Koch, de que la internet tendría la capacidad de sentir y hasta de albergar conciencia. Según esto, el enfoque de la Singularidad Tecnológica[13] que es la capacidad que tienen las maquinas con inteligencia artificial para automejorarse podría ser un argumento para la teoría de Koch a la que ya he brindado explicación.

Si por el lado de Koch se realizaba la hipótesis antes mencionada, por el lado de Herbert Marshall McLuhan anterior a este, predeciría la internet con 20 años de antelación, por ese entonces, el principio de los sesenta. El diría que el medio que llegase sería la extensión de la conciencia.

Muchos de sus escritos fueron dedicados a los medios digitales y de comunicación. Se refirió a los medios electrónicos diciendo que la asidua demanda de su uso, recuperaría la conciencia tribal o grupal que se convertiría, además, de ser unos grupos pequeños a ser una extensión inimaginable formando una “aldea global”[14]. Este pensamiento traería implicaciones mayores, al punto de concebir así mismo, la idea de una “conciencia global”.

Sus palabras marcaron huella contundente al decir: “En lugar de dirigirse hacia una vasta librería de Alejandría, el planeta se ha convertido en una computadora, un cerebro electrónico, como una obra de ciencia ficción infantil, al exteriorizarse nuestros sentidos, el Gran Hermano se asienta en nuestro interior. (para referirse a la conciencia que se vería colonizada por un sin número de ideas que posiblemente no son de nuestro pensamiento).

“Así que, a menos de que seamos conscientes de esta dinámica, nos moveremos hacia una fase de terrores de pánico, adaptándonos a un mundo pequeño de

[12] WIKIPEDIA. [sitio web]. Red neuronal artificial [Consulta: 20 octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Red_neuronal_artificial

[13] CCCBLAB. [sitio web]. La singularidad [Consulta: 20 octubre 2021]. Disponible en: https://lab.cccb.org/es/la-singularidad/

[14] BBC. NEWS. [sitio web]. Marshall McLuhan, el "profeta de la era digital" que predijo internet 20 años antes de que se inventara [Consulta: 20 octubre 2021]. Disponible en: https://www.bbc.com/mundo/noticias-40681655

tambores tribales, interdependencia total y coexistencia superpuesta".[15] (para referirse a la convivencia con otras culturas que traerán otro sentido, nuevas ideas que sino desplazan a las nuestras, habremos de adoptarlas y entremezclarlas para matizar con distorsión a las que ya teníamos, una nueva cultura impura, ejemplo de ello, tenemos los americanismos, los rasgos culturales africanos y europeos en nuestra identidad cultural).

Eh aquí otra de las implicaciones, como resultado daría una consecuencia que hasta hoy produciría escozor, y que es la razón de este trabajo, en sus palabras al referirse a la internet: "Una vez que hayamos supeditado nuestros sentidos y sistemas nerviosos a la manipulación privada de quienes intentarán beneficiarse a través de nuestros ojos, oídos e impulsos, no nos quedará ningún derecho."[16]

Y como si esto fuera poco, se encontró algo muy parecido a lo de aldea global de la que hablaba más adelante de cómo es el mundo virtual. Este término apareció en 1985 cuando una inspiradora empresa dedicada a la industria del entretenimiento llamada Lucas-Arts[17] Entertainment Company, más conocida como Lucas Film, y cuyo dueño era George Lucas, dedicado a la ciencia computacional, crea el primer mundo virtual realizando un entorno que tiene como nombre hábitat diseñado en 2D y que constaba de avatares escogidos por los jugadores para luego poder realizar acciones que ya estaban plenamente configuradas y programadas. Pero ¿Qué es un mundo virtual? Un mundo virtual, es eso, una creación meramente virtual que tiene como base el mundo real, se crea con fines educativos por ser de alto impacto en quienes interactúan con esta herramienta y debido a ello se fueron convirtiendo en juegos. ¿Existe conciencia en este mundo (en el mundo virtual)? Es claro la direccionalidad de este mundo virtual y su intensión socio-comercial, pero como juegos no tienen o no se les ha programado para establecer conciencia en razón a que se extralimitan para causar alguna dependencia por lo cual los hace "exitosos", en conclusión, la conciencia en este mundo virtual es nula cosa que pone en riesgo especialmente a la juventud que juego a juego pueden ver como su forma de pensar se va modelando en la interacción con este tipo de mundo virtual, malo o bueno, ese impacto establece un parecer en nuestra juventud.

4.1.2 Teoría del Conectivismo

Esta teoría surge en la era digital como un resultado concienzudo de los científicos George Siemens (1970 canadiense) y Stephen Downes (1959 canadiense) haciendo referencia a la tecnología en la era digital que marco un ambiente globalizado para explicar cómo los seres humanos se comunican, aprenden y viven,

[15] Ibid
[16] Ibid
[17] STARWARS.FANDOM. [sitio web]. Lucas Arts [Consulta: 20 octubre 2021]. Disponible en: https://starwars.fandom.com/es/wiki/LucasArts

a su postura teórica se le conoce más como "teoría del aprendizaje para la era digital"[18] donde el punto de partida es el mismo ser humano.

Ya de por sí, la era digital desbordo al ser humano que es el punto de partida y un elemento que evidenciaría el laberinto indiscutible en su estrecha relación con esta tecnología. El conectivismo sin duda desenredaría la “pita” y aportaría bases para entender un poco el advenimiento de la conciencia en relación con esta era. Si bien la saturación de aprendizajes frecuentes, conceptos, el mundo como una incógnita, era una realidad y basados en el conectivismo, se dedujo que entonces, se debería gestionar tal conocimiento conscientemente bajo una reflexión constante, sería la forma de decantar la unión entre aprendizaje, experiencia y conocimiento. Los internautas están siempre formando su pensamiento con conocimiento independiente de si ese conocimiento sea bueno o malo, la concienciación sería el punto clave para esta era digital que promocione una conexión más erudita, pensada y reflexiva.

No cabe duda de que este conjunto de redes y nodos formados por estos sistemas digitales tienen una profunda implicancia sobre los principios de los seres humanos ya que al establecer los enlaces o conexiones se produce la supervivencia en un mundo y por efecto de la conectividad globalizado en cuyo aprendizaje dejó de ser personal y que además lo define.[19]

4.1.3 Pandora (II) y el Nuevo Paradigma de Ciberseguridad[20]

Como quiera que se llame, el ciberespacio, el espacio virtual, la internet, las TICS conforman un entramado de tecnología, pero también de instrumentos para el aprendizaje y el conocimiento del ser humano. Este espacio que es eminentemente virtual se le asimila a la caja de pandora de la que al abrirla se liberaron toda clase de males y por los cuales hemos de adaptarnos o tan siquiera no ser conscientes de ello. Nada tan cierto como la evolución de esta tecnología que avanza a pasos extremadamente agigantados, pero nada más cierto que no hay una correlación entre esa evolución y su seguridad. Por el momento las soluciones han sido meramente técnicas e inacabadas y aunque mucho se ha pensado al respecto, aunque hay mucho proyecto y muchos estudios, podríamos decir que cada persona al ingresar al ciberespacio tendría prácticamente que convertirse en un corta fuegos para crear un entorno seguro.

---

[18] Siemens, George. [sitio web]. «Connectivism: A Learning Theory for the Digital Age». International Journal of Instructional Technology and Distance Learning 2. https://jotamac.typepad.com/jotamacs_weblog/files/Connectivism.pdf

[19] WIKIPEDIA. [sitio web]. Conectivismo [Consulta: 20 octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Conectivismo

[20] INDRA. [sitio web]. Pandora (II) y el nuevo paradigma de Ciberseguridad [Consulta: 20 octubre 2021]. Disponible en: https://www.indracompany.com/es/blogneo/pandora-ii-paradigma-ciberseguridad

4.1.4 ¿Por qué será que, al Producirse una Agresión en Sistemas, se Avivan las Conciencias?[21]

Una razón, quizá la más centrada y real, es que en el mundo en forma globalizada ha puesto atención en razón a que la industria del cibercrimen no descansa y por tanto es un momento clave para aprovechar y realizar toda clase de campañas para que aprendamos a usar todo nuestro potencial en torno a la protección personal y los activos de la información cuando trabajamos para una empresa que podemos poner en riesgo cuando entramos a esta caja de pandora que es el ciber espacio.

Solo necesitamos de una red que nos conecte al ciberespacio para ser hackeados, dice Marc Asturias, Senior director de Fortinet[22] (es una empresa proveedora para la seguridad en la red y como empresa son lideres mundiales en gestión contra amenazas). Marc, dice que es responsabilidad de los estados adelantar todas las campañas posibles para evitar caer en las manos de la cibercriminalidad y generar una concientización ya que el radio de acción de los hackers tiende a ampliarse con plena profesionalización de su modo de actuar.

4.1.5 ¿Cuándo Sabemos que hay una Conciencia Digital, Conciencia Cibernética o Ciber Conciencia?

Cuando las personas toman las precauciones necesarias para no caer en la trampa del ciber delito. Actualizar el sistema en forma continua cada vez que el sistema se lo pida, contraseñas difíciles de detectar, dar forma a la privacidad en redes sociales y no tramitar información relevante por este medio, usar un antivirus, *(entre otras)* sería la forma de darse cuenta de que hay concienciación en ciberseguridad.

4.1.6 Los Ciber-Cooperantes[23]

Un nuevo concepto de concientización dirigido a toda la sociedad que ha impulsado -INCIBE- El Instituto Nacional de Ciberseguridad. Este es un programa que se ha popularizado con éxito en España y que podría claramente tener repercusión en Colombia de darse, está realizado por voluntarios (quinientos profesionales al momento) que hacen llegar su voz con el concepto de concienciación a niños, adolescentes, padres de familia, docentes en el uso consciente del ciberespacio y más precisamente en las redes sociales.

Como es posible que junto con la evolución de la tecnología evolucionen todos los males que salen de esta caja de pandora llamada ciberespacio, se empieza a ver

[21] SYNEIDIS. [en línea]. La necesidad de construir una conciencia social sobre ciberseguridad [Consulta: 20 octubre 2021]. Disponible en: https://www.syneidis.com/es/social-conscience-cybersecurity/
[22] Ibid
[23] Ibid

como la sociedad globalizada o esta aldea global empieza a despertar y se va formando un nuevo paradigma, basado en la ética, la responsabilidad y la conciencia a manera de escudo contra los males de la ciberdelincuencia.

4.1.7 El Ciberespacio Concebido como Conciencia Mundial

McLuhan había prevenido la venida de la internet con antelación y había asegurado que el medio que viniera sería la extensión de la conciencia. Hoy en la era moderna cuando la tecnología alcanzó una gran evolución, se propone al ciberespacio como conciencia mundial. Y es que ese entramado de redes, nodos y conexiones que se dan entre humanos por medio del ciberespacio y del ser humano con la maquina y de la maquina con el mundo hasta el punto de convertirla en un lugar para el aprendizaje, la gestión del conocimiento y un lugar de encuentro. Este espacio virtual como tecnología ha ido creciendo y aprendiendo del ser humano como nos lo dice la teoría del conectivismo. Una sola cultura, un pensamiento, una cultura que se va estructurando con el aporte y retroalimentación de cada ser humano que recibe pero que también aporta conocimiento para ir consolidando una conciencia mundial con el contexto del ciberespacio como herramienta para que se de este hecho.[24]

4.2 MARCO HISTÓRICO

"…vengo del Ciberespacio, el nuevo hogar de la Mente…" escribía **John Perry Barlow** en su Declaración de Independencia del Ciberespacio en Davos, Suiza el 8 de febrero de 1996[25] ya hace veinticinco años. Kosch en su teoría del conectivismo nos muestra como el aprendizaje tiende a globalizarse, McLuhan proyectándose a la tecnología venidera diría que esta se convertiría en la extensión de la conciencia. Ellos veían un gran poder desarrollándose que traería fuertes implicaciones para la vida del ser humano al punto de pensar al ciber-espacio como una aldea global.

Todos estos atributos y entre muchos otros hoy reposan sobre el concepto de ciberespacio. Y durante décadas ha soportado aplausos, críticas y enemistades. Etimológicamente hablando de la palabra ciber espacio, su prefijo viene de un concepto mucho más antiguo que es cibernética que se desprende del griego kibernetike cuyo significado se restringe al arte de navegar[26]. Este mismo significado será empleado por el escritor William Gibson en el año 1984 en su

[24] REVISTA MARINA. [en línea]. El ciberespacio y su impacto en el orden social pág. 135 [Consulta: 20 octubre 2021]. Disponible en: https://revistamarina.cl/revistas/2013/2/gomez.pdf
[25] BIBLIOWEB. [en línea]. Declaración de Independencia del Ciberespacio [Consulta: 20 octubre 2021]. Disponible en: https://biblioweb.sindominio.net/telematica/manif_barlow.html
[26] UV.ES. [en línea]. Ciberespacio y protección de los derechos [Consulta: 20 octubre 2021]. Disponible en: https://www.uv.es/cefd/5/lima.html

famosa novela “Neuromante”[27] cuando mencionó la palabra “ciber-nao” para referirse a pilotear una nave.

Cuando nace la internet, se instaura el ciber espacio. La internet surgió en el año 1969 en EE. UU. como una necesidad de independizarse del ordenador central y conseguir ser menos vulnerable por lo cual se crea ARPANET (Advanced Research Projects Agency - Agencia de proyectos de investigación avanzada) que surge en medio de la guerra fría para lograr un mejor ambiente a las comunicaciones de su ejército[28].

En 1973 se desarrollan tanto sus protocolos como el control de transmisión. 1980 fue un año clave porque entonces la internet deja de tener un interés militar, motivo por lo cual pasa al manejo de las agencias por su interés científico. En Europa, el interés fue otro, ahí se vio potencial y captó un interés académico mediando el ambiente universitario, cinco años después todas las universidades estaban intercomunicadas, en 1989, el científico Tim Berners-Lee, desarrolla World Wide Web (www)[29] que es una infraestructura que ordena la información en internet, información que se produce en un espacio eminentemente virtual y por tanto en el ciberespacio.

4.2.1 Estado Actual

La sociedad en general debería preguntarse: Creo que todos deberíamos preguntarnos, ¿Qué tan vulnerable es la sociedad frente al ciberdelito? Vasta tan solo con tener un celular, una Tablet, un computador, IoT entre otros y tener acceso virtual para comprobarlo. Mas que cierto, es saber que la mayoría de los cibernautas desconocen o evitan precauciones al momento de navegar en el ciberespacio, todo parece que el ansia de saber, conocer, encontrar, comprender, obnubila el pensamiento y se manda al traste alguna precaución que se haya atendido. La vulnerabilidad, es un hecho que se hace patente cada día más y descubre con preocupación que tanta importancia le concede el ciudadano de a pie como la misma industria que tanto mal ha recibido de esta tendencia tan negativa que se ha convertido en un cáncer para el mundo en general.

Como ya hemos dicho antes, el ciberespacio es netamente virtual y como tal, no concede fronteras, en este espacio cabe todo un mundo de posibilidades entre las que cuentan los ciberdelitos que representan un peligro para los cibernautas y que

[27] BBC. [en línea]. ¿Cómo llegamos al ciberespacio? [Consulta: 20 octubre 2021]. Disponible en: https://www.bbc.com/mundo/noticias/2016/03/160316_origen_palabra_ciber_finde_dv
[28] MIRA COMO SE HACE. [en línea]. ¿Qué es, para qué sirve y cómo funciona el Arpanet? – Historia del Internet [Consulta: 20 octubre 2021]. Disponible en: https://miracomosehace.com/que-es-para-que-sirve-como-funciona-arpanet-historiainternet/#%C2%BFQu%C3%A9_es,_para_qu%C3%A9_sirve_y_c%C3%B3mo_funciona_el_Arpanet?_%E2%80%93_Historia_del_Internet
[29] Ibid

adoptan nuevas tendencias, procedimientos y como el tiempo en el ciberespacio les facilita estar en todo el planeta estableciendo redes delictivas que operan en un abrir y cerrar de ojos.[30]

4.2.2 El Ciberdelito a Nivel Mundial

La ONU, estima que la cantidad de víctimas en el mundo por el ciberdelito alcanza al millón. Así mismo se dice que los hackers en el mundo cuentan ya ochenta millones y que el delito transnacional afecto aproximadamente a cuatrocientos mil personas según el docente en derecho de la universidad UNAM[31]. La delincuencia organizada se nutre con las tres cuartas partes de esos delincuentes que llegan a catorce personas por segundo según la ONU.[32]

El también académico de la UNAM, Rodolfo Romero Flores, consideró que el ciberdelito a nivel mundial representa un dos por ciento del PIB, los países con más desarrollo un diez y seis por ciento y los menos desarrollados un treinta seis por ciento[33], dicho a manera de síntesis.

4.2.3 El Ciberdelito en Colombia

En el anterior subtitulo pudimos ver una síntesis clara de la forma que ha tomado el mundo en cuanto a la ciberseguridad se trata y que trae fuertes implicancias para una tecnología que no se merece tal tratamiento y tal fama pues en su fondo tiene grandes virtudes de las cuales se surten los cibernautas que la exploran con motivaciones como las del conocimiento.

Pero, en el mundo el ciber delito es una lucha cotidiana, en Colombia la realidad no es muy diferente. Se encontró que de enero a marzo del 2021 los ataques cibernéticos tuvieron una escalada del treinta por ciento, según aseguro la fiscalía general de la Nación[34] (como se explica en el grafico a continuación y de acuerdo con las estadísticas del 2020).

---

[30] INTERPOL. [en línea]. Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. [Consulta: 20 octubre 2021]. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

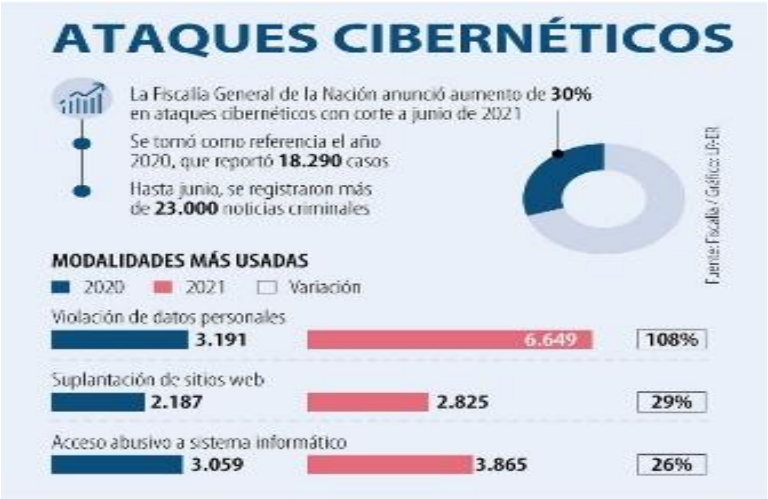
[31] UNAM. [en línea]. Boletín UNAM-DGCS-943 Ciudad Universitaria. [Consulta: 20 octubre 2021]. Disponible en: https://www.dgcs.unam.mx/boletin/bdboletin/2021_943.html

[32] Ibid.

[33] Ibid

[34] ASUNTOSLEGALES. [en línea]. Los ataques cibernéticos aumentaron 30% durante el primer semestre de este año según la Fiscalía. [Consulta: 20 octubre 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

Ilustración 1. Estadística Ataques Cibernéticos



Fuente: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

Pero de Colombia las dos ciudades que más ataques de este tipo fueron en primer lugar Bogotá con ocho mil trecientos cincuenta y cinco episodios y Medellín con 1664.[35]

De lo anterior podemos analizar: una es la capital de Colombia que aloja el palacio presidencial y es el centro del país donde se mueven fuertemente los negocios porque ahí se encuentran representadas muy importantes empresas de la industria del país y la otra es la ciudad textil del país y al igual que la capital se encuentran grandes empresas que mueven la moda y el negocio textil. Como se muestra en el cuadro a continuación: de la generalidad de casos, los más representativos son Bogotá, Medellín, Cali, siendo las más destacadas las dos primeras. Esas podrían ser las razones del porque tengan el más grande auge de este delito y que llama el olfato de los ciberdelincuentes que ven en estas ciudades potencial para asentar su radar malicioso en torno a negocios de gran envergadura.

[35] Ibid.

Cuadro 1. Ataques Cibernéticos en Colombia

ORIGEN	TIEMPO	MODALIDAD	INCIDENTE/DELITO CASOS	INCREMENTO PORCENTAJE
Colombia	2020	generalidad	18.290	
Colombia	Corte a junio 2021	generalidad	23.000	25.7%
Bogotá	2021	Local/generalidad	8.355	
Medellín	2021	Local/generalidad	1.664	
Cali	2021	Local/generalidad	1.569	
Situación	2021	violación de datos personales	6.649	108%
Situación	2021	suplantación de sitios web	2.825	29%

Fuente: GAVIRIA RESTREPO, Jorge Ivan. Basado en Ataques Cibernéticos en Colombia Fiscalía Gral. de la Nación

Durante la pandemia la escalada fue del cincuenta y cinco por ciento más comúnmente por ciber-delito, fraude y hurto.

4.3 MARCO CIENTÍFICO O TECNOLÓGICO

Lo que hoy hemos denominado tecnologías digitales ha sido categórico para los seres humano en el transcurso de la historia y de la pandemia que, para evitar sus efectos más directos, ha sido de gran ayuda este recurso para poder efectuar multiplicidad de operaciones como intercambios bancarios, recibir clases en modo virtual, comunicación virtual, pago de servicios, compras virtuales, uso de bibliotecas virtuales, aplicativos virtuales, en fin.

Si queremos entrar en comunicación con el mundo lo que se debe hacer es entrar a internet o en su defecto navegar en el ciberespacio, todo acceso al ciber espacio comienza entrando por la internet.

4.3.1 Una Tecnología que Sorprende

¡Si!, esta tecnología sorprende, navegar en el ciber espacio es toda una experiencia cultural, didáctica y de aprendizaje, hasta el punto de que su tecnología trae consigo novedosas acciones que son necesarias para la instrucción del usuario, por ejemplo, algunas destacadas:

- Una de las cosas que se debe hacer para tener participación en internet es tener una dirección electrónica, esta es un código que se hace importante que cada cibernauta lo adquiera.

- Para acceder a los multiservicios que ofrece el ciberespacio se debería adquirir de acuerdo con la necesidad el equipo correcto, lo que le permitiría claridad sobe el lenguaje usado de la conexión para la comunicación entre computadores donde es el modem el medio transmitiendo por línea telefónica.

- Esta conexión, esta soportada por la enorme red formada por ordenadores que es lo que define en definitiva a la internet que con todos los medios informáticos que posee logra conectar a más de 1.5 millones de ordenadores en el globo terráqueo.

- Internet lo que antes era ARPANET (creado en 1969)[36], tenía como fin ayudar a los investigadores que vivían en la tensión de la guerra fría entre Rusia y EE. UU. En 1983 se amplió sus redes de ordenadores para operar desde las regiones.

- Hoy internet ha crecido descomunalmente con la ampliación de sus redes facilitando la labor investigativa de académicos, científicos, estudiantes universitarios entre otros y pueden entrar a uno u varios computadores en forma remota por intermedio de un remote Access Software (software de acceso remoto).

- Otro recurso muy válido para obtener información es la ciber-media que es comunicación interactiva, su nombre es una conjunción de las teorías de Norbert Wiener y de Marshall McLuhan[37], es así como esta comunicación es posible entre seres humanos, seres humanos y ordenadores, ordenadores a ordenadores.

- La ciber-media es una gran posibilidad para tener acceso al ciber-espacio y obtener toda la información que se pueda encontrar ya que es especial para la búsqueda periodística y su difusión. Gabriel Alejandro Elizondo Ramírez[38] que es un importante académico, aseguró que el ciber-medio es el cuarto

[36] SCIELO. [en línea]. Como fuente de referencia académica. [Consulta: 20 octubre 2021]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762001000200002

[37] Ibid.

[38] UNIVERSIDAD TÉCNICA DE BABAHOYO. Difusión de contenido multicultural en los nuevos medios
DIGITALES ECUATORIANOS. [en línea]. [Consulta: 20 octubre 2021]. Disponible en: http://dspace.utb.edu.ec/bitstream/handle/49000/8832/E-UTB-FCJSE-CSOCIAL-000324.pdf?sequence=1

medio de comunicación que ha permitido que los medios tradicionales estén involucrados en medios digitales.

Algunas características del Ciber-medio son: multimedialidad, hipertextualidad, actualización, interactividad.

1. Multimedialidad: se puede entender también como multiplataforma, es la unión de distintos medios de comunicación dentro del hipertexto. Generalmente este concepto es muy identificado con contenido para la difusión especialmente se adapta con rigurosidad al periodismo por su versatilidad y capacidad multitarea.[39]

2. Hipertextualidad: el estadounidense Theodor Holm Nelson filósofo y sociólogo fue quien acuñó este nombre en relación con la *internet y el ciberespacio* para anexarlo a la lectura interactiva y no lineal dentro del carácter de la informática. El hipertexto es un sistema con el cual se pueden relacionar fracciones de textos entre sí.[40]

3. Actualización: se refiere a la información que en el periodismo es importante debido a que las noticias no son hechos estáticos sino dinámicos, acá una cosa lleva a la otra en cuanto a reacciones, consecuencias, desarrollos, además, estos medios son referencia tanto local como mundial.

4. Interactividad: hace referencia a la comunicación y la relación que hay entre emisor y receptor en cuanto al intercambio de posibilidades que solo se da en los medios con los cuales se concibe la reciprocidad y la retroalimentación. Es un flujo y devenir de información que da pie tanto a la creatividad como a las ideas.[41]

La evolución del ciberespacio no ha parado, hoy se puede presenciar como las redes sociales están en pugna por la lucha de obtener más cibernautas para que naveguen bajo su influjo, redes que ofrecen más seguridad, más información cultural y de entretenimiento porque es una industria que mueve mucho dinero ya que en apariencia es “gratis”. Por otro lado están en boga las aplicaciones digitales que son una gama amplia actuando en el ciberespacio ofreciendo toda clase de contenido dinámico, unos para entretenimiento, otras son operacionales para ayudar a la gente a crecer en diferentes facetas de la vida como son los cursos de idiomas, otras son ayudas al campo, otras ayudan a gente a ubicarse en un territorio, otras ayudan a la cuestión de la cocina, entre muchas otras y con la afluencia de un gran público por su facilidad de manejo y comprensión. Facebook con su crecimiento exponencial hoy da un paso más de modernidad que nos tiene

[39] UMA. [en línea]. Qué se entiende por multimedialidad. [Consulta: 20 octubre 2021]. Disponible en: https://www.uma.edu.ve/postgrados/periodismo/revista_nro3/Multimedialidad.html
[40] SIGNIFICADOS. Tecnología e Innovación [en línea]. [Consulta: 20 octubre 2021]. Disponible en: https://www.significados.com/hipertexto/
[41] PENTA3. [en línea]. Qué es interactividad [Consulta: 20 octubre 2021]. Disponible en: http://penta3.ufrgs.br/midiasedu/modulo6/etapa1/biblioteca/interactividad.pdf

a la expectativa de la cual se supone un amplio crecimiento que se ofrecerá a quienes frecuentan estas redes con el llamado metaverso, amanecerá y veremos.

4.3.2 Panpsiquismo

Mientras la hipótesis de la *singularidad tecnológica del científico Raymond Kurzweil* (Queens, Nueva York, 12 de febrero de 1948) con especialización en las ciencias de la computación e IA[42] dice que un robot, un ordenador, la misma red de internet, el ciberespacio, tendrían la capacidad de establecer sus propias mejoras contando para ello con sus propios recursos llegando incluso con esto a superar la misma inteligencia humana[43], el panpsiquismo de cuyo exponente más relevante fue Arthur Eddington, cuya teoría dice que, cualquier materia ya sea animada o inanimada es capaz de tener algún grado de conciencia[44]. Esta sorpresiva noticia, para persona comunes y corrientes, que ya había sido lanzada con antigüedad nos enseña entonces que la conciencia no sería propia de los seres humanos, sino, que este rasgo es compartido con las cosas, por ejemplo, con el ciberespacio y hasta la misma internet.

Así mismo, la teoría de la información integrada (IIT) dice que un sistema podrá llegar a cierto grado de integración de la información y pueda alcanzar una phi que pase de cero, lo que haría pensar que ese sistema tiene algún grado de conciencia[45]. La posición de esta teoría es otra, aunque parecida ya que, si acepta la presencia de conciencia, pero condicionada a que ese sistema independiente del que fuera debería tener una phi mayor a cero para albergar algún grado de conciencia.

Esta noción del l panpsiquismo a la cual se han unido físicos, matemáticos, filósofos ya sea para aseverarla, criticarla o rechazarla, como se ve, ha sido muy dinámica y es así como pasa por muchas corrientes y posturas dejando una estela de razonamientos.

Lo que debe quedar claro al momento es: que el panpsiquismo pasa por muchas teorías que intentan explicar el problema de la conciencia y en lo que al tema respecta es que el asunto digital y como se ha visto en el marco teórico, podría tener conciencia, ahora un apunte que llama la atención es que la mente como

---

[42] WIKIPEDIA. [en línea]. Raymond Kurzweil [Consulta: 20 octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Raymond_Kurzweil

[43] Ibid.

[44] BBC. [en línea]. Panpsiquismo: cómo es la teoría de que todo, desde una roca hasta una casa, tiene conciencia (y por qué gana credibilidad académica) [Consulta: 20 octubre 2021]. Disponible en: https://www.bbc.com/mundo/noticias-42904290

[45] CIENCIA UNAM. [en línea]. La conciencia como información integrada [Consulta: 20 octubre 2021]. Disponible en: http://blogs.ciencia.unam.mx/paradigmaxxi/2015/05/03/la-conciencia-como-informacion-integrada/

tal, aborda la posibilidad que es ubicua, es decir, que está en todas partes, dicho de otra forma, en el universo[46]

4.4 MARCO LEGAL

Como ya se ha reiterado en contadas formas sobre el crecimiento exponencial de las TICs y su grado de tecnología, ha sido de gran provecho para la nación porque implica el desarrollo comercial, social y cultural. Pero, así como le caben todos los atributos históricos, sociales, económicos y culturales también, se puede decir que ha sido de provecho para la ciber-delincuencia que ven en el ciber espacio una oportunidad para "exprimir" ese mundo que representa la virtualidad y de qué forma. Hoy la ciberdelincuencia por su forma de obrar y sin ningún cartón que lo avale, ha logrado tal grado de sofisticación en la forma de operar para obtener un usufructo mal habido.

Históricamente se conoce quizá el primer intento de ataque cibernético o sino uno de los más importantes, el realizado, no se sabe el origen, realizado a Arpanet en EE. UU. en su departamento de defensa. Se llegó a decir que su sistema extrañamente los mensajes titilaban y los códigos cambiaban sin razón aparente. Se involucró a los ingenieros del momento que dieron solución al hecho pasado 3 días.

Los técnicos altamente calificados en ciberseguridad realizaron un antivirus para dar fin a la situación.[47] El cibercrimen fue creciendo cada día más y amplio sus tentáculos y para contrarrestarlos varios países implementaron una norma judicial especial a la cual se unió Colombia en el año 2009.[48] En un principio los virus se transmitían por medio de disquetes, luego fue en forma virtual y esto sirvió para crear protocolos y enfrentarlos. Entonces encontraron otro medio que fue la USB. A medida que se iba volviendo tendencia el ciber delito, se les fue enfrentado a la medida de su crecimiento. En Colombia se dice que la respuesta fue más bien tardía o lenta debido a que hacerles frente implicaba realizar inversiones cosa que no les cayó bien a los directamente perjudicados. Debido a esto las respuestas fueron y siguen siendo lentas por el mismo motivo.[49]

El especialista en asuntos penales Alberto Suárez Sánchez define el ciber delito como un acto por medio de herramientas informáticas para cometer un ilícito en

[46] WIKIPEDIA. [en línea]. Pampsiquismo [Consulta: 20 octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Pampsiquismo
[47] SCIELO. [en línea]. Delitos informáticos y entorno jurídico vigente en Colombia. [Consulta: 20 octubre 2021]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003
[48] Ibid.
[49] Ibid.

detrimento de terceros y para afectar la información como el bien jurídico que representa.[50]

Las leyes que rigen o pretenden proteger los activos informáticos son:

4.4.1 Ley 1273 de 5 de Enero 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 (Diario Oficial nº 47.223).[51]

- **Ley 269I**, se refiere al hurto utilizando medios informáticos o por lo menos semejantes a estos[52].
- **Ley 269J**, sobre la transferencia de información sin el permiso debido[53].
- **En 2016 - Varsovia/OTAN** el ciber espacio es reconocido como un dominio de operaciones junto con la tierra, el aire, el mar[54]
- **Sujetos del ciber espacio:** corresponde a las personas, el personal de carácter ideal o jurídicas.[55]
    - También son quienes se conectan para recibir y dar contenido
    - Las personas que brindan servicios o bienes
    - Las personas jurídicas, físicas, privadas, públicas,

4.4.2 Declaración de Independencia del Ciberespacio

- Es un precioso documento, (Davos, Suiza el 8 de febrero de 1996 por John Perry Barlow) una obra artística, por la forma tan real, pero a la vez un grito en el que hay un proceso de empoderamiento legítimo de alguien que siente al ciberespacio como diría Barlow, la nueva casa de la conciencia.

---

[50] Ibid.
[51] INFORMATICA-JURIDICA. Legislación Informática de Colombia. [en línea]. [Consulta: 20 octubre 2021]. Disponible en: https://www.informatica-juridica.com/legislacion/colombia/
[52] POLICÍA NACIONAL. Normatividad sobre delitos informáticos. [en línea]. [Consulta: 20 octubre 2021]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Art%C3%ADculo%20269I%3A%20Hurto%20por%20medios%20inform%C3%A1ticos%20y%20semejantes.&text=El%20que%2C%20con%20%C3%A1nimo%20de,sancionado%20con%20pena%20m%C3%A1s%20grave.
[53] Ibid.
[54] WIKIPEDIA. [en línea]. Ciberespacio. [Consulta: 20 octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Ciberespacio#Origen_del_t%C3%A9rmino
[55] Ibid.

- Es una petición, demanda en contra de la injerencia de los poderes que arriesgan la virtualidad como un espacio de encuentro social y cultural reclamando la soberanía del ciber espacio.[56]

- El texto comienza así: “Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente…”[57]

- Y termina así: “Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes.”[58]

[56] Ibid.
[57] UHU. [en línea]. Declaración de Independencia del Ciberespacio. [Consulta: 20 octubre 2021]. Disponible en: http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf
[58] Ibid.

5 DESARROLLO DE LOS OBJETIVOS

La expresión CIBER DEFENSA, obedece básicamente a una estrategia cuya meta es un mejoramiento en seguridad con respecto a todo lo que concierne al ciber espacio. Es toda una inquietud que se plantea como un tema especial y predilecto del que se obtienen grandes resultados. Así mismo, se relaciona en este espacio, referencias o títulos que diferentes autores han tratado acerca del tema que acá se aborda, retroalimentado, fortaleciendo y empoderando el nivel de conocimientos en función de este trabajo y que constituye el estado del arte a manera de respaldo y soporte para el mismo:

5.1 DESARROLLAR UNA REVISIÓN DE ESTADO DE DEL ARTE CON AL MENOS 20 REFERENCIAS ACADÉMICAS SOBRE LA CIBERDEFENSA EN LAS ORGANIZACIONES.

Cuadro 2. Referencia Académica 1

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo ▪ Articulo	García Forero, Luis Felipe Guillermo ▪ 2020	Fortalecer a la organización en la seguridad de la información	Las empresas realizan onerosas inversiones en su arquitectura de ciberseguridad, pero, no así invierten en la concienciación de su personal, que es potencialmente un eslabón muy vulnerable constituyéndose en un inminente riesgo para el manejo y manipulación del activo sensible y vital que es la información.
Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2c%20el%20personal.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 3. Referencia Académica 2

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
El INCIBE británico (NCSC): «Las personas pueden ser el eslabón más fuerte en ciberseguridad.» ▪ Articulo	KYMATIO ▪ 2018	La seguridad de la información ha sido liderada por la tecnología, pero no se ha relievado el rol y el valor que constituyen los profesionales	Potenciar, reforzar, capacitar, relievar el rol y valor de los profesionales (para la empresa) que trabajan en la cadena-relación-usuarios son la verdadera solidez de TI y por tanto de la ciberseguridad, esto les pondrá en contraposición al paradigma de ser el eslabón más débil y les permitirá ser un activo de seguridad dinámico, visible y contundente
Disponible en: https://blog.kymatio.com/es/el-incibe-britanico-ncsc-las-personas-pueden-ser-el-eslabon-mas-fuerte-en-ciberseguridad/			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 4.Referencia Académica 3

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Comparativa de empresas sobre la concienciación en ciberseguridad ▪ Video	INCIBE ▪ 2015	Desarrollar una cultura de seguridad y preparar al personal	La concienciación es un recurso que debe ser parte de las políticas de TI de la organización, siendo así la normativa una herramienta visible y palpable de una cultura de la seguridad como resultado de una capacitación dirigida a los buenos resultados que se traduce en un alto nivel de seguridad
Disponible en: https://www.youtube.com/watch?v=Y6vO2HxrEPc			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 5. Referencia Académica 4

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
CONCIENTIZACIÓN / 44% de los usuarios sufrió un incidente de seguridad a través del correo electrónico ▪ Articulo	CIBERSEGURIDAD LATAM ▪ 2022	El correo electrónico como vector de propagación de amenazas informáticas	ESSET, empresa líder en detección de amenazas cibernéticas el día "mundial del correo", evidencia las perspectivas de seguridad en que se encuentra el correo electrónico como vector de ataques y engaños a usuarios desprevenidos. *Un clic más consciente puede hacer la diferencia* entre una empresa más segura (en lo concerniente a la ciberseguridad) y la ingeniería social.
Disponible en: https://www.ciberseguridadlatam.com/2019/10/16/44-de-los-usuarios-sufrio-un-incidente-de-seguridad-a-traves-del-correo-electronico/			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 6. Referencia Académica 5

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
BANCOS / Las nuevas modalidades de vishing, smishing y fishing con las que hacen fraude bancario ▪ Articulo	La Republica ▪ 2022	El activo de información es asediado por las variaciones en las tendencias de cibercrimen que buscan engañar a la banca	Las tendencias en ciberestafas han ido cambiando y se cierne una nueva modalidad para la que rara vez se está preparad@ utilizando para ello medios de comunican que hoy nos facilitan el trabajo y en Colombia la ingeniería social ha dado cuenta de la banca que ha sufrido mucho con esta tendencia de cibercrimen que busca ávidamente una decisión de la victima
Disponible en: https://www.larepublica.co/finanzas-personales/las-nuevas-modalidades-de-vishing-smishing-y-fishing-con-las-que-hacen-fraude-bancario-2969016			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 7. Referencia Académica 6

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
TENDENCIAS CIBERCRIMEN COLOMBIA 2019 – 2020 ▪ Informe PDF	POLICIA Nal, DIJIN, CCIT, TICTAC, SAFE ▪ 2020	El avance de la cibercriminalidad se da por el gran nivel en que accionan sobre sus víctimas y por el desconocimiento de las empresas de como estos operan	Las políticas definidas en que se relacione la gestión de los roles y responsabilidades son muy importantes para llegar a una acción efectiva de seguridad y que sirva para recuperar la operatividad en caso de concretarse un ataque. En Colombia el cibercrimen va en alza conectándose con cierta facilidad al dispositivo de los usuarios desprevenidos que tienen relación de alguna manera con la banca donde pulula lun dañino agente como lo es el programa maligno
Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 8. Referencia Académica 7

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
La ciberseguridad política clave dentro de las organizaciones ▪ Tesis	González Díaz, David Leonardo, Pulido Sainea, Saúl Sebastián ▪ 2021	El control interno como parte importante de las políticas y ciberseguridad para su fortalecimiento frente al cibercrimen	El desconocimiento o inconciencia de la ciberseguridad como la contratación de personal no idóneo y precaria normatividad en las empresas de Colombia donde el control (que debiera ser el eje rector para el buen desempeño de la ciberseguridad) no es el fuerte, hace de dichas empresas una meta vulnerable para el cibercrimen
Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/37635/2021davidgonzalezsaulpulido.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 9. Referencia Académica 8

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Incidencia del factor humano en la seguridad de la información de las organizaciones públicas de categoría 6. ▪ Monografía	Fernández, Luis Jonalber ▪ 2020	El ser humano de entidades gubernamentales en desconocimiento de la ciberseguridad e intromisión de terceros, es pieza fácil frente al cibercrimen	Ya sea por el alto nivel de rotación, desconocimiento de la ciberdefensa, inconciencia, entre muchas otras, que se tipifica una alta deficiencia de entidades gubernamentales frente a la sofisticación dirigida acorde a intereses del cibercrimen que ronda en forma persistente y se hace grandes éxitos en ataques a estructuras gubernamentales vulnerables.
Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/38893/ljfernandez.pdf?sequence=3&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 10. Referencia Académica 9

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES ▪ Tesis	Romero Castro, Martha Ireney otros ▪ 2018	El control frente a especificidades y categorizaciones internas en las fases de reconocimiento y detección de vulnerabilidades	Cuando el control hace parte de las políticas empresariales y es además un método para acceso a la información sensible, es una herramienta eje que transversaliza la empresa en su fortalecimiento para el empoderamiento de la ciberdefensa
Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 11. Referencia Académica 10

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia* ▪ Informe/Articulo	Milton Ricardo Ospina Díaz y otros ▪ 2020	A pesar de la ciber técnica alcanzada en Colombia para empoderar la ciberdefensa, se vislumbran vulnerabilidades frente al desafío mundial	Un recorrido histórico de la ciberdefensa hasta nuestros días para observar la situación, avances y retrocesos desde lo gubernamental en Colombia frente al mundo, evidenciando los desafíos que tiene con los ciber peligros
Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7667839			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 12. Referencia Académica 11

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA ▪ Tesis	Pérez Pérez, Yuly ▪ 2017	Bajo el marco del CONPES, Colombia moderniza la ciberdefensa para salvaguardar la economía en diferentes frentes mediante planes y plazos y objetivos a cumplir	Mediante la gestión de la ciberseguridad y en el marco de CONPES Colombia se emplaza a fortalecer el camino que lleva a una gran ciberdefensa mediante un proceso de implementación de la seguridad informática para constituir alertas tempranas que coadyuben en su fortalecimiento y mitigación del riesgo
Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 13. Referencia Académica 12

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Prevención en ciberseguridad enfocada a los procesos de infraestructura tecnológica ▪ Informe	Mauricio Rodrigo Cando-Segovia y otros ▪ 2021	Se pone en perspectiva, por medio de una documentación seria y objetiva el statu quo de la ciberdefensa en Colombia y Latinoamérica poniendo de manifiesto las vulnerabilidades existentes	Se aglutina el resultado de la literatura de diferentes autores que buscan radiografiar la situación de la ciberseguridad en Colombia y Latinoamérica (y por extensión al mundo), bajo la visión empresarial de como la infraestructura relacionada a la tecnología aun es muy pobre con respecto a los retos que se tienen en el espectro de la ciberdefensa, lo que constituye una especie de llamado de atención a todos los entes tanto gubernamentales como empresariales
Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7888164			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 14. Referencia Académica 13

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Recomendaciones para prevenir ciberataques ▪ Informe	Alsina Rodríguez, Juan Manuel ▪ 2015	Se hacen recomendaciones que parten del conocimiento de la forma como el ciberdelincuente opera para conseguir su propósito	Las vulnerabilidades son el pan de cada día y es aceptada como algo normal sin que existan las prevenciones hasta que se concretan, muchos interrogantes aparecen entonces como medida para dar solución al asunto que parte desde la implementación de políticas que coadyuben en el fortalecimiento de dicha seguridad. En el documento se relacionan recomendaciones que a manera de pedagogía dan la noción de los aprendizajes básicos para prevenir el acto de programas maliciosos sobre el activo de la información
Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2922/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 15. Referencia Académica 14

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
La falta de conciencia, una vulnerabilidad latente para la seguridad de la información ▪ Ensayo	Zambrano Granada, Dayhann Geraldynn ▪ 2019	La falta de conciencia de los usuarios y de la empresa, es y ha sido la causa del éxito y avanzada de los ciberdelincuentes, más sin embargo existe la norma y/o estandarización con la cual se puede repeler las amenazas	Se relieva que el punto más débil en el ciberespacio son los usuarios que contrasta con la educación al respecto sin la cual se hace presa fácil del ciberdelincuente para obtener información, pero son las entidades las responsables y las que deben matizar los pormenores del asunto para no dar lugar a la explotación. Son las entidades las que deben ponerse en salvaguarda frente a la normatividad existente
Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2922/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 16. Referencia Académica 15

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Seguridad informática y seguridad de la información en el mundo, como factor de enseñanza en Colombia ▪ Tesis	Parra, Carlos Humberto ▪ 2015	El advenimiento de la internet trajo consigo tanto progreso como problemas que impactaron al mundo y hoy se necesita implementar inteligentes modelos para salvaguardar el activo más importante tanto de una nación como de una empresa que es la información y Colombia no es la excepción	Un ciber ataque es una acción disruptiva que ha puesto al mundo en vilo, siendo los países más desarrollados los que a lo largo de la historia han encontrado en técnicas, orden, políticas, estandarización, gobernanza, entre otros, la forma de enfrentar el tema y en Colombia esta experiencia ha servido como tema de enseñanza (es uno de los países en Latinoamérica que más ha avanzado en el tema de ciberseguridad) aunque la inconciencia, falta de capacitación y de gestión son elementos claves que hacen de las empresas tanto privadas como públicas adolezcan de muchas vulnerabilidades y por tanto peligre la información.
Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2856/00002352.pdf?sequence=1			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 17. Referencia Académica 16

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Actualidad de Colombia en seguridad de la información ▪ Trabajo de Grado	González Hernández, Edwin Mauricio ▪ 2014	Una radiografía que destaca alcances, desafíos y logros por cumplir de Colombia dentro del escenario mundial	Si bien es cierto, Colombia ha superado el pensamiento del subdesarrollo al enfrentar con decisión el desafío de la modernidad y poner su imagen dentro de la esfera mundial como un país que lucha por obtener logros en este campo, también es cierto que aún falta y más cuando la sociedad en la que vivimos (desde la misma empresa hacia abajo) hace movimientos que redundan en la falta de conciencia que no permite un avance más rápido
Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2882/Trabajo%20de%20grado1886.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 18. Referencia Académica 17

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Administración del riesgo cibernético un enfoque desde la alta gerencia empresarial en Colombia ▪ Ensayo	Riveros Cárdenas, Fredy Orlando ▪ 2017	La administración del riesgo como un tema que la alta gerencia debe empoderarse pues es quien tiene el poder de respuesta y la visión holística para establecer las soluciones con una mirada más amplia, precisa y contundente	Es una admirable visión desde algunos pensadores, entre ellos Mc Luhan, que han dado enormes contribuciones al mundo e invitan a ver el panorama de la internet desde un punto de vista más positivo y consecuente llamando la atención sobre la cibernética como una ciencia que puede darnos mucho, pero al fin y al cabo que vislumbró un mundo con falta de preparación para la modernidad. Así mismo toca el tema de la administración del riesgo como un eje que proveerá soluciones inteligentes organizadas, meditadas, sabias para matizarlo y solucionarlo.
Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/15837/RiverosCardenasFredyOrlando2017.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge IvanCuadro

19. Referencia Académica 18

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia ▪ Monografía	Peralta Cuadrado, Mary Luz Roa Ibarra, Eduardo Enrique ▪ 2021	El apogeo de la internet ha revolucionado la forma de hacer negocios y el ciber espacio es una herramienta que le permite al comercio, quizá por la inmediatez, grandes retribuciones, pero matizadas por la ciber seguridad	Cuando se habla de internet, el riesgo siempre será un tema eje, solo que es abordado desde las operaciones comerciales realizadas en el ciberespacio. Estas operaciones fueron impulsadas con el COVID 19 y van en alza cada día más por la forma en que Colombia le dio respuesta a la situación y como el ofrecimiento de la reserva de los datos conquistó al público. También las empresas en dichas operaciones le han dado un frente común al riesgo y han sabido solventar con gestión y administración tanto el riesgo como las soluciones.
Disponible en: https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/3949/EL%20IMPACTO%20DEL%20DELITO%20CIBERN%c3%89TICO%20EN%20LAS%20OPERACIONES%20DE%20COMERCIO%20ELECTR%c3%93NICO%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 20. Referencia Académica 19

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Operaciones cibernéticas y seguridad hemisférica en Colombia: análisis desde la cooperación regional e internacional. ▪ Ensayo	Guerrero Vallejo, Gina Yuleisi ▪ 2022	Una visión desde las organizaciones internacionales con sus documentos dentro del marco histórico y del derecho transnacional y la postura de Colombia como una respuesta cierta ante el dilema de la ciber seguridad	Se hace un recorrido histórico teniendo como centro la multidimensionalidad que tiene el hemisferio con respecto a la seguridad electrónica y el impacto que causa la estrategia mundial desde las organizaciones internacionales (por intermedio de documentos) en Colombia y como nuestro país da respuestas a la incertidumbre que producen las amenazas cibernéticas en todos los niveles de la sociedad
Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/42878/2022ginaguerrero.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 21. Referencia Académica 20

TÍTULO DE LA PUBLICACIÓN Y TIPO DE DOCUMENTO	AUTOR (ES)	IDEA CENTRAL	RESUMEN
Ciber estrategia Colombia ▪ Articulo	Nova Alarcón, Michael Alejandro ▪ 2016	Análisis valorativo de la seguridad y de la ciber defensa de Colombia con el criterio y mirada OTAN	Una visión a partir de documentos de organizaciones internacionales y regional apoyada en características históricas importantes como parte del análisis valorativo, teniendo como propuesta central estrategias con miras a la integralidad cibernética donde se hacen diversas evaluaciones que buscan el bien social y económico
Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/14171/MichaelAlejandroNovaAlarcon2016.pdf?sequence=1&isAllowed=y			

Fuente: GAVIRIA RESTREPO, Jorge Ivan

5.2 DESARROLLAR UN ANÁLISIS DE LOS RESULTADOS OBTENIDOS DE LA REVISIÓN DEL ESTADO DEL ARTE.

5.2.1 Análisis de Resultados - Estado del Arte

5.2.1.1 Objetivo de la Revisión:

Dicha revisión se realiza para asumir el alcance con determinación frente al trabajo que se realiza. Esto muestra una capacidad de empoderamiento del tema pues la expresión ciber conciencia es difícil de hallar y aunque fue menester la deducción hoy más que nunca con esta revisión aparecen documentos que se refieren a la concienciación como eje de solución o de estudio y análisis orientado a la ciberseguridad.

5.2.1.2 Tipo de Evaluación:

Esta evaluación es descriptiva, porque detalla un breve resumen radiográfico de la referencia obtenida, tipo de documento, fecha de publicación, autor, idea central a manera de síntesis.

5.2.1.3 Delimitación:

- Se evaluaron referencias que datan del año 2015 hasta el 2022. Se observó artículos con *vigencia* interesantes desde esa fecha a la actual *constatando*, que muchas cosas que se decían desde el 2015 aún se dicen en textos

actuales, *lo que configura un progreso lento de modernización tanto de la infraestructura técnica como la conceptual cibernética*.

- Se evaluaron textos enfocados en Colombia pero que pueden estar matizados por el panorama de Latinoamérica o mundial o viceversa, el panorama latinoamericano o mundial que impacta el statu quo de Colombia. O el resto del mundo como referencia para saber cuánto se retrocede o progresa.

5.2.1.4 Tendencia:

- Hay una tendencia marcada al referirse a palabras que se constituyen como *palabras clave* que repiten constantemente los autores como son: gestión, políticas, vulnerabilidad, modernización, procesos, administración, ciber seguridad, activos de información, concienciación, en algunos textos se deduce a las personas como un activo de la ciberseguridad por el valor que se le da, y que recogen el alma del análisis.

- Otros textos enmarcan el proceso de "ciber modernización" como resultado de la globalización o la globalización como un ente que catapulta tanto retrocesos (*por la problemática generada*) como avances (*el advenimiento que causa la internet en la esfera económica mundial y regional enmarcando una nueva cultura del pensamiento*).

- Algunos textos les fue necesario hablar del asunto en cuestión haciendo un paso por la historia con la necesidad de observar el proceso que ha tenido el país con respecto a Latinoamérica y el mundo. Es así como se llega a decir que Colombia está en el quinto lugar de los países latinoamericanos con más ataques cibernéticos causados. También se enumera a Colombia para decir que este país con respecto al resto del continente tiene enormes progresos.

5.2.1.5 Valoración de la Calidad:

- Las referencias asumidas se apoyan en estadísticas de importantes medios y encuestas realizadas por empresas que trabajan en ciberseguridad según la revisión de sus bibliografías, gráficos con referencias, documentos estudiados y referenciados.

- Las referencias evaluadas generalmente son documentos de los cuales se observó un buen soporte bibliográfico.

- Las referencias tomadas van desde artículos incisivos, monografías que abordan el tema con profundidad, informes de análisis hasta tesis universitarias.

5.2.1.6 Desarrollo de Temas:

Cuadro 22. Análisis Desarrollo de Temas Estado del Arte

Estado del Arte	Desarrollo de Temas del Estado del Arte		
	Datos Relevantes	**Alcance**	
Documentos	Importancia de la ciberseguridad en Colombia (Tesis)-Pérez Pérez Yuly - 2017	Propenden por el uso de documentos producidos por organismos internacionales para apoyar una postura seria, critica y categórica bajo el marco de ley y/o estandarización como fuente de soluciones soportadas por estudios previos y buenas prácticas. Esto los hace más interesantes porque establecen un contraste sabio y determinante con respecto a otros trabajos que sin usarlos desglosan una serie de soportes investigativos desarrollados para expresar un pensamiento	
	Prevención en ciberseguridad enfocada a los procesos de infraestructura tecnológica (Informe) - Mauricio Rodrigo Cando-Segovia y otros -junio 2021		
	Operaciones cibernéticas y seguridad hemisférica en Colombia: análisis desde la cooperación regional e internacional (Ensayo)-Guerrero Vallejo, Gina Yuleisi - 2022,01,27		
	Ciber estrategia Colombia (Articulo) -Nova Alarcón, Michael Alejandro -2016,03,23		
Administración	Seguridad informática y seguridad de la información en el mundo, como factor de enseñanza en Colombia (tesis) -Parra, Carlos Humberto -2015,07,23	Estos trabajos dan un gran valor a la categorización y proponen la administración como un ente con poder de decisión y visión holística con la que perciben soluciones por el grado de experiencia y solidez en la gestión del riesgo	
	Administración del riesgo cibernético un enfoque desde la alta gerencia empresarial en Colombia (ensayo) -Riveros Cárdenas, Fredy Orlando -2017,01,31		
Concienciación / Conciencia	Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo (articulo)-García Forero, Luis Felipe Guillermo -2020	Concientización / 44% de los usuarios sufrió un incidente de seguridad a través del correo electrónico (articulo) -Ciberseguridad LATAM -17, mar, 2022	Es un tema recursivo en estos trabajos que hacen hincapié en la necesidad de capacitar al empleado aún más en conciencia que determina una capacidad del rol que desempeñan porque el ciber atacante se surte de tal vulnerabilidad o inexistencia de esta herramienta de valor que bien aprovechada les permite poner su atención en los procesos que se desarrollan en la cotidianidad con efectividad
	El INCIBE británico (NCSC): «Las personas pueden ser el eslabón más fuerte en ciberseguridad.» (articulo) -KYMATIO -17, agosto, 2018-2020	La ciberseguridad política clave dentro de las organizaciones (tesis)-González Díaz, David Leonardo, Pulido Sainea, Saúl Sebastián -21, sep,2021	
	Comparativa de empresas sobre la concienciación en ciberseguridad -video -INCIBE -7, sep., 2015	La falta de conciencia, una vulnerabilidad latente para la seguridad de la información (ensayo) -Zambrano Granada, Dayhann Geraldynn -2019	
Historia	Administración del riesgo cibernético un enfoque desde la alta gerencia empresarial en Colombia (ensayo) -Riveros Cárdenas, Fredy Orlando -2017,01,31	Estos documentos hacen un repaso por la historia trayendo para recordar procesos, consecuencias, modernización, retrocesos y avances significativos demandando tanto al ente empresarial como gubernamental y social apropiarse de la capacitación y conocimiento para seguir el proceso con contundencia	
	Seguridad informática y seguridad de la información en el mundo, como factor de enseñanza en Colombia (tesis) -Parra, Carlos Humberto -2015,07,23		

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Resultados del Análisis:

- Si da el valor a los roles que el profesional desempeña dentro de la empresa llámese gubernamental, privada o mixta, no se tendría que enfocar el personal como eslabón vulnerable, sino como un activo de seguridad. Este tema se hace importante al tocar el eje rector que es la búsqueda de la conciencia como factor determinante para fortalecer la seguridad empresarial y ciberdefensa

- Colombia ha sido determinante en el proceso de gestionar el riesgo y pudiera parecer que frente a las estadísticas falta mucho camino por recorrer si no fuera por la ciberdelincuencia que se ha tomado su trabajo muy en serio y sus ataques diarios pasan de miles con los cuales logran sus objetivos, estos ataques realizados así de una manera incisiva terminan por minar la técnica por un lado y por otro, la confianza de los usuarios que son asediados por intermedio del correo electrónico, teléfono y otros

- Es claro que Colombia ha realizado un papel importante en los esfuerzos por defender la economía como un ente fácil para reportar dividendos. Pero, son las personas desde el de a pie, hasta los entes empresariales privados y gubernamentales que deben concientizarse de su labor de salvaguardar la información, pero el primer respondiente según se analizó en el estado del arte, es la empresa, porque de ella deben provenir las soluciones, las capacitaciones, la escogencia del personal calificado, apegarse a la normatividad vigente y proporcionar el camino para realizar el proceso.

- La gestión del riesgo este pilar una vez establecidos los objetivos, hace todo lo que esté a su mano para su logro, lo que constituye una consecución/gestión) y la administración (en este pilar se establecen los controles preventivos que son: evitar, detectar, recuperar, lo que configura una alerta temprana y de mitigación de la vulnerabilidad) son dos pilares importantes que sostienen los procesos de mejora frente a la ciberseguridad.

- El panorama de la ciberseguridad puede ser otro: provocando un pensamiento distinto en el personal calificado valorando cada rol como un eslabón de fortaleza, empoderándolo y abriéndole un camino atencional donde su clic cotidiano se haga ético, concienzudo y verdaderamente profesional apegado a la normatividad y/o lineamientos.

- El camino que Colombia ha asumido frente a la gestión del riesgo debe traerle grandes compensaciones porque ha hecho todo lo que debe hacer, otra cosa es que cada ciber nauta se piense y se sienta con un alto valor como humano y ayude al país en los logros que tiene por cumplir, es decir,

la sociedad debe inmiscuirse aún más y considerarse parte del proceso para mitigar el riesgo con el cual la economía estará siempre minada

5.3 DISEÑAR UNA ESTRATEGIA DE CIBERSEGURIDAD PARA LAS EMPRESAS PÚBLICAS Y PRIVADAS DE COLOMBIA BASADO EN LA ISO 27002

Para dar respuesta a este propósito es importante llegar a unas consideraciones que son de vital importancia para poder establecer un direccionamiento estratégico integral. Para tal efecto se sugiere una perspectiva profunda enfocada en **la madurez empresarial** (como inicio) que se vislumbra como una filosofía de trabajo o modelo eficaz para construir progreso. El desarrollo de este propósito esta realizado desde **la premisa de la concienciación** que involucra **a las personas** como parte del eslabón que la ingeniería social usa para llegar a su objetivo que son los activos de información, datos y otros más asociados.

- Nota:

- **Este diseño estructura en esencia, un modelo** que busca ser alcanzado por empresas colombianas de cualquier nivel que descubriendo la necesidad de concienciación en ciberseguridad, podrán tener la oportunidad de salvaguardar sus activos informáticos de una forma metódica y adentrarse a un sistema de actividades estándar concretas que le permitan a la empresa su empoderamiento en dicho tema y la oportunidad de expandir su actividad económica, ya que puede ofrecer ese plus (seguridad en el intercambio de datos)El diseño propone el modelo de madurez que determina el estado en que se encuentra un posible alcance en ciberseguridad y capacidad para enfrentar una implementación de dicho tipo, en cuyo caso, le permite una visión holística de gestión que acceda a soluciones integrales, asimiladas a un todo estructurado
- El diseño de ciberseguridad para las empresas públicas y privadas de Colombia se basa en la ISO 27002:2022 porque, además, es un estándar que aplicado le permite un nexo seguro con cualquier empresa que tenga como meta la ciberseguridad
- Aunque este diseño basado en la ISO 27002:2022 no busca que la empresa se certifique, porque ese no es lo que se busca como alcance, su implementación si le ayuda a una posible certificación.
- El diseño basado en la ISO 27002:2022 busca en específico el énfasis en las buenas prácticas. La empresa deberá asumir las que necesite de acuerdo a su estado o nivel en que se encuentre.
- No se busca diseñar sobre lo diseñado, se busca con el modelo logrado, un modelo facilitador para la gestión de la ciberseguridad en las empresas públicas y privadas de Colombia

5.3.1 ¿Qué es la Madurez Empresarial?

Aunque la madurez empresarial no es una cortapisa o norma rígida para cumplir, si es una autogestión importante que demanda el statu quo y por ende la **actitud/aptitud** concluyente de auto mejoramiento con el que se piensa y apunta a una meta siempre mejor, por eso sugiero saber los niveles de madurez empresarial de los datos como estrategia, ya que le permite a la empresa una evaluación honesta, legitima y singular.

La madurez empresarial (que no puede sobrar en ningún esquema de evaluación) y para el caso nuestro desde los datos/información, se conoce como **un ejercicio autónomo integrador de mejores prácticas** que definen la estructura de un plan ascendente cotidiano y consecutivo, medible y cuya asimilación es una orientación donde se estructura la renovación del ente institucional. Aunque puede ser fácil decir cual pudiera ser el nivel de madurez por lo que se percibe, lo que dice su estado de prioridades es otro ya que esto solo se consigue con una evaluación pormenorizada, detallada y consecuente. No se pretende dar acá una guía de cómo realizar este valioso ejercicio más si dar luz conciliadora que una todas las partes integrantes del órgano empresarial.

5.3.2 ¿Por qué se hace importante saber el nivel de madurez empresarial?

- Muestra su capacidad para dar respuesta integral desde lo tecnológico.
- Mide la capacidad de respuesta y capacidad como empresa.
- Muestra la aptitud para adaptarse a las tendencias comerciales.
- Muestra la actitud para la mejora constante y persistente.
- Determina la evolución, proyección/dirección, gestión empresarial.
- Muestra la capacidad de gestión y vislumbra el crecimiento.
- Muestra tanto la vocación y orientación (visión).
- Es un plus que promueve valor hacia el cliente.
- Mide/evalúa el rendimiento.
- Valora la implicancia/consecuencias del estado actual con respecto al estado optimizado.
- Permite un nivel de mejora profundo y es por eso por lo que llega a ser un fuerte soporte para futuras implementaciones.
- Establece una mejora continua y de todos los procesos.
- Mide el alcance empresarial y para el caso acá tratado, la gestión, administración y mejoras en la protección de los activos de información.
- Muestra todos los esfuerzos por identificar la madurez tecnológica con el fin de hacer los procesos más agiles y más eficientes.

La gestión de la madurez empresarial es una gran oportunidad y virtud que genera un buen impacto para implementaciones posteriores por que genera una profunda evaluación en la que se evidencia y se hace visible tanto la pertinencia como los posibles riesgos de la organización, ya sean muchos, una cantidad razonable o pocos de acuerdo con el "tamaño" empresa, pero nunca dejan de ser riesgos, *así* sea uno, pueda ser de cuidado y poner en jaque a la empresa. Entonces, su implementación deberá ajustarse/remediar de forma óptima/integral, el pedido y/o necesidad de mejora que se ha identificado en dicha evaluación y que llevará a la madurez empresarial. La madurez empresarial es una plataforma ideal tanto para el desarrollo como para el crecimiento empresarial.

Estos tres factores constituyen el enfoque del nivel de madurez empresarial:

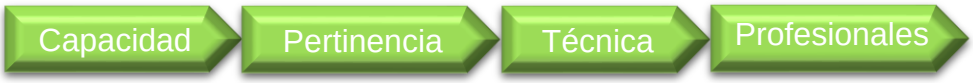
- **Coherencia:** Este factor determina la credibilidad. Se muestra la capacidad como un valor que alinea el enfoque organizacional, propende por resultados y muestra el empoderamiento para establecer logros.

Ilustración 2. Madurez Empresarial Factor de Coherencia

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Habilidad: Este factor determina el grado de implementación y el grado de adaptabilidad de este. Se muestra la actitud proactiva como un agente que se orienta al cambio, capaz de resolver "nudos problémicos" con habilidad y creatividad, gestionando siempre positivamente hacia resultados concretos y determinantes.

Ilustración 3. Madurez Empresarial Factor de Habilidad



Fuente: GAVIRIA RESTREPO, Jorge Ivan

- **Compromiso:** Este factor determina el grado de seriedad y visión. *El compromiso acá se convierte en una estrategia* que posiciona a la empresa frente a la sociedad para la se labora. Se denota el interés de los diversos agentes en forma transversal por el cumplimiento, el deber, la respuesta pertinente, el grado de unión, el fin y el rol como agentes vitales y además visionarios.

Ilustración 4. Madurez Empresarial Factor de Compromiso

Fuente: GAVIRIA RESTREPO, Jorge Ivan

Cuadro 23. Modelo de Niveles de Madurez de la Información

Nivel	Explicación
(1) INICIAL	▪ No se conoce proceso de análisis de dato alguno ni CDI (Calidad de los Datos de la Información). La seguridad de la información es básica. La información/datos no se valora como un activo esencial.
(2) DEFINIDO	▪ Se tiene presente la minería, visualización, herramientas e infraestructura de datos de manera básica. La calidad/seguridad de los datos de la información es observada sin evaluación/análisis por lo que no hay interés de mejora y solución a problemas.
(3) INTEGRADO	▪ Se ha introducido una base de datos que se evidencian por la documentación realizada y consultada. Se afronta los problemas de calidad/seguridad de datos solo que se actúa al respecto una vez sucedido el hecho problémico no antes (no preventivo)
(4) GESTIONADO	▪ Se conocen procesos de Inteligencia de Negocios que evidencian documentación y consulta. El estado de la calidad/seguridad de la información se evalúa/analiza con frecuencia para su posterior ajuste.
(5) OPTIMIZADO	▪ Se conocen procesos de Inteligencia de Negocios que evidencian documentación y consulta. El estado de la calidad de la información se evalúa con frecuencia para su posterior ajuste estableciendo la mejora continua. La información/datos tienen un valor esencial y por tanto se evidencia su cuidado y aseguramiento.

Fuente: Basado en Scielo. Modelos de Madurez en los Datos de una Organización. [septiembre 2012]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892012000200004

Los modelos de niveles de madurez informática, como el caso acá expresado en la imagen anterior, es una autogestión considerada desde **la conciencia de la necesidad de mejora** para impactar la infraestructura organizacional como al cliente a quien por fin le llega el producto final. Redunda en la Inteligencia de Negocios, inteligencia comercial o BI en la que la gestión mejora los procesos internos midiendo los rendimientos y optimizando el equipo y/o herramienta inmersa en los cambios. **Las escalas que muestra la imagen, es una visión**

administrativa del problema que describe objetivamente la etapa en que se puede encontrar la empresa y el proceso a que se ve abocado a cumplir para poder escalar la mejora. Este proceso, se orienta desde la necesidad de la empresa, políticas y objetivos trazados.

La finalidad de la norma: ISO 27002 es tener presente el conocimiento de los activos que se poseen, información que debe hacer parte de la gestión/administración de riesgos.

Cuadro 24. Norma ISO 27002

Nivel: Condición/Criticidad/Rigor	Aseguramiento en Calidad de
Confidencialidad	▪ Acceden a la información solamente las personas que estén autorizadas
Integridad	▪ Su tratamiento y desarrollo derivan de la exactitud y la completitud
Disponibilidad	▪ Tanto la información como los activos asociados están disponibles a la orden del día

Fuente: GAVIRIA, Jorge Ivan

Al observar la propuesta/estrategia de seguridad (cuadro abajo final), se podrá evidenciar **que los controles de seguridad obedecen a estos tres niveles (confidencialidad, integridad y disponibilidad)** que define la seguridad de la información en cuatro dominios: los controles organizativos, los controles de personas, los controles físicos y los controles tecnológicos.

Cuadro 25. Conceptos Relevantes en la Implementación de la ISO 27002

Función	Acción
Gestión de Incidentes	▪ proceso para restaurar los servicios TI/sistema que han sufrido alguna interrupción
Manejo de no Conformidades	▪ un proceso desde el sistema de calidad para que un requisito no aceptado sea gestionado desde la legislación en forma oportuna
Gestión Documental	▪ realizado desde las normas técnicas para administrar la documentación: elaboración, revisión, aprobación
Administración de Riesgos	▪ acciones alineadas para responder/gestionar manejar la incertidumbre que producen los riesgos ante los objetivos de una organización
Mejora Continua	▪ revisión/análisis continuo de operaciones/procesos para optimizar el escalamiento del progreso
Análisis de Causa	▪ acción/análisis que busca precaver/prevenir la reincidencia problémica al identificar sus precedentes
Plan de Acción	▪ programa/guía encaminado a acciones en: tiempo, modo y lugar
Activo	▪ un recurso empresarial esencial fijo/corriente y/o asociado con gran valor en el proceso de producción
Implementación	▪ acción/ejecución de la puesta en función de operaciones programadas/planeadas, es una gestión del proyecto
Control de Acceso	▪ garantía autorización/restricción del acceso lógico/físico a los activos de información
Activo	▪ "algo" que tiene un valor esencial para la empresa/organización - en TI un activo primario: información/datos
Vulnerabilidad	▪ característica asociada a cualquiera de los activos que por detalles de calidad/controles en su seguridad pudiera ser explotado/vulneración por una/varias amenazas(s) (físicas, lógicas, estratégicas)

Fuente: GAVIRIA, Jorge Ivan

5.3.3 Estrategia de ciberseguridad para las empresas públicas y privadas de Colombia basado en la ISO 27002

La estrategia no global más si especifica (buenas prácticas/**controles**) que se sugiere a continuación y como lo dice el propósito, es tanto para empresas públicas como privadas. Cabe decir, que esta no es una guía rigurosa de implementación (es una estrategia basada en controles que se deben escoger de acuerdo con la necesidad de la empresa/organización), es una estrategia de ciberseguridad (basada en la ISO 27002 y sus buenas prácticas, observa por medio de controles todo el ambiente que rodea a la ciberseguridad de una u otra forma) donde pueden acudir todo tipo de empresas que estén interesadas en salvaguardar los activos, especialmente los de información/datos.

Cuadro 26. Estrategia Ciberseguridad Empresas Públicas y Privadas

Característica	Sector Público	Sector Privado
Disponibilidad	▪ opera con alto grado de disponibilidad que cuidan de proteger	▪ rigurosamente restringida a personal no esencial por la confidencialidad
Software	▪ está limitado al cumplimiento de ciertas operaciones ▪ el soporte de los sistemas y de los desarrolladores es limitado, *aunque* puede darse por contrato	▪ se opera de acuerdo con el cumplimento de roles ▪ cuentan con el soporte de los sistemas y desarrolladores en cualquier momento
Parches de Seguridad	• no es una opción ni recibirlos ni actualizarlos porque cualquier cambio puede generar problemas en toda la operación • puede restringir la alta disponibilidad de aplicarse	• es una opción válida para algunas situaciones/errores sucedidos en el sistema • la disponibilidad puede afectarse por un lapso siendo solucionado por dpto. TI.
Datos	• los datos e información hacen parte del sistema integrado del estado para realizar tareas tanto cuantitativas como cualitativas que tienen que ver con la ciudadanía	• los datos e información son el eje de la empresa como un activo esencial que le permite planificar los movimientos a nivel de negocio/comercio
Trazabilidad	• se mide para valorar el alcance de las políticas de estado • los procesos sistemáticos son eminentemente administrativos	• se valora para observar los procesos que permiten los rendimientos esperados • los procesos sistemáticos hacen parte de las políticas de la alta gerencia

Fuente: GAVIRIA, Jorge Ivan

5.3.4 Estrategia del Propósito

Es importante aclarar: la ISO 27002:2022 es un estándar respaldo que complementa a la ISO 27001, esta característica no la hace certificable, pero si ayuda a la certificación.

El siguiente cuadro, es la respuesta concreta al propósito tres que consta de:

- **Dos sugerencias:**
  - Una sugerencia basada en el modelo de madurez informática, ya explicada arriba más ampliamente.
  - Una sugerencia que tiene que ver con la ISO 27002:2022/**controles: inteligencia de amenazas** y que aún no ha sido publicada porque está en proceso, la considero necesaria para adoptarla ya que es una

respuesta casi científica a la modernidad de los ataques con los que se enfrenta la empresa pública como privada en el día de hoy.

- **Una estrategia basada en las buenas prácticas/controles de la nueva ISO 27002:2022**
    - La estrategia deriva en que solo toma controles (esenciales) para la ciberseguridad. Generalmente cuando se hace una implementación se tiene en cuenta la ISO 27001 como base de certificación, acá no se tiene en cuenta porque el enfoque está en los 4 dominios de controles más dos sugerencias para establecer objetivos entre los que está el empoderamiento, fortalecimiento de la ciberseguridad mas no la certificación.
    - Una estructura con cuatro dominios de controles esenciales que a su vez se diversifica y potencia en otros, más específicamente como un desarrollo del dominio. En total son 93 controles actualizados de 114 de la pasada edición. No tiene sentido trabajar con una ISO desactualizada porque en este momento las empresas que han implementado antes la norma ahora mismo tienen que estar en el proceso de transición de la actual.
- **La ventaja que se tiene de realizar un diseño de ciberseguridad informática basada en controles:**
    - Se equilibran los procesos de seguridad y se establece un sistema administrativo de gestión que los coordina entre sí.
    - Se propende por un método que contribuye a la mitigación/reducción del riesgo.
    - Incrementa y armoniza todos los niveles de seguridad de una forma integral.
    - Establece altos niveles de responsabilidad que permite en forma determinante la concienciación.

- Tres marcos de seguridad de la información/datos. Los otros dos marcos se encuentran armonizados en los controles que llamo esenciales por su nivel de importancia. Esos dos restantes entran a especificar y caracterizar lo ya descrito en el marco controles.

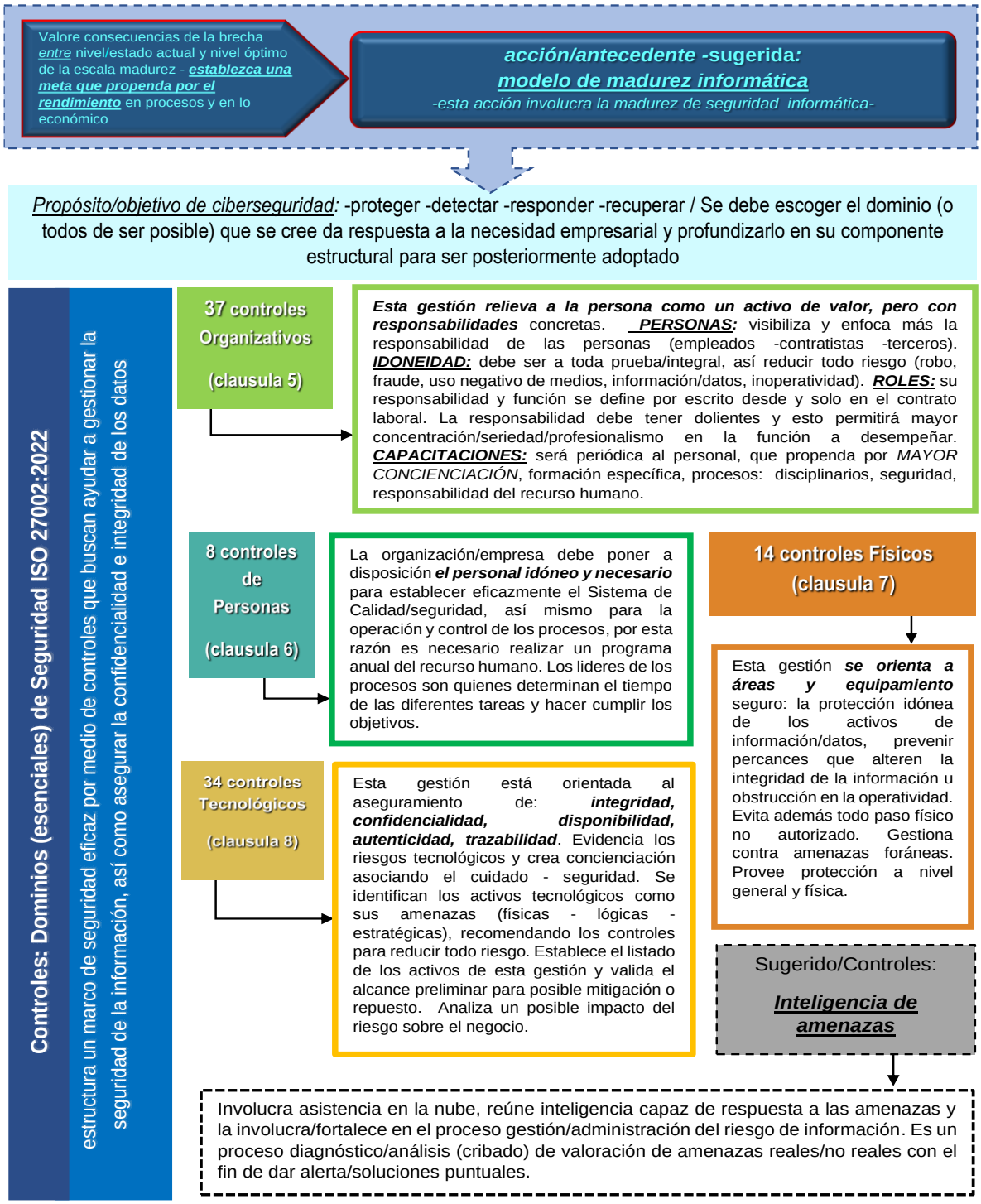
- **Marcos Controles:**
    - Presentados en cuatro dominios base de implementación que son los que trabajamos como estrategia. Hay 11 nuevos controles que no son dominio más se presentan como temas. Estos temas se adentran en la especificidad, pero ya se tratan en los cuatro dominios, por eso no

entran en la estrategia. De estos solo se asume como relevante uno que es INTELIGENCIA DE AMENAZAS.

- **Marcos Programa:**
  - Precisa requisitos con los cuales configurar el sistema de seguridad de la información.

- **Marcos Riesgo:**
  - Precisa el proceso de gestión de riesgos.

Ilustración 5. Estrategia de ciberseguridad para las empresas públicas y privadas de Colombia basado en la ISO 27002



Fuente: Basado en la Norma ISO 27002, Diseño Estrategia por GAVIRIA, Jorge Ivan

6 CONCLUSIONES

Se desarrolló una revisión del estado del arte con 20 referencias académicas sobre la ciberdefensa en las organizaciones de Colombia y se destaca a manera de conclusión, que si bien es cierto, que los ataques se han extendido como un virus a nivel mundial, también es cierto que en el abordaje local, se encontró entre otros y de manera especial, la falta de conciencia cibernética que se tipifica como un descuido o falta de preparación profesional (capacitación) en lo que concierne al accionar laboral donde el personal es asediado de muchas formas, por ejemplo, con técnicas intrusivas como el vishing, smishing y fishing.

Se desarrollo un análisis de los resultados obtenidos de la revisión del estado del arte sobre la ciberdefensa en las organizaciones de Colombia desde las cuales donde se pudo evidenciar que, si el personal que trabaja para la empresa se asume como un activo humano y esencial, se le capacita, empodera y fortalece, dejará de ser parte de la vulnerabilidad palpable que puede servir de entrada a los ataques cibernéticos. La concienciación es un eje esencial que tiene sus raíces desde el proyecto y no en la improvisación o cuando se hagan reales las amenazas, Colombia ha presentado lucha contra el problema de la ciberseguridad basado en dos pilares: la gestión y la administración del riesgo soportado desde la cooperación internacional.

Se diseñó una estrategia de ciberseguridad para las empresas públicas y privadas de Colombia basada en la ISO 27002, las empresas pueden desarrollar su propio esquema de ciberseguridad basados en cualquiera de los protocolos avalados por los diferentes gobiernos y a nivel internacional, siempre y cuando tengan la capacidad de proteger todos sus niveles de relación comercial por intermedio de las acciones que designe la formalidad adoptada, ya que un esquema pobre e improvisado puede dar como consecuencia el efecto dominó abriendo puertas para la intrusión tanta in situ como a las empresas de relación transaccional. Una ciberdefensa soportada por controles es muy eficaz para detener, denegar, restringir el acceso tanto al espacio físico como al espacio lógico empresarial donde el ciberdelito se encuentra con un esquema ciber-seguramente pensado, probado, armonizado e integral. Una estrategia de diseño de ciberdefensa es por extensión una estrategia de concienciación, donde los parámetros están supeditados a las capacidades de desarrollo y abordaje de las diferentes piezas protocolarias, que propenden por la seguridad de los activos empresariales por parte del personal.

7 RECOMENDACIONES

- Entender la problemática de la concienciación programándola en la estructura de la implementación, debe ser una tarea seria, estratégica, administrativa (planificar) y eminentemente de gestión.

- Considerar la capacidad de lo humano como activo esencial sin perder la objetividad ni desvirtuar la norma para empoderar el rol y el profesionalismo frente a las vulnerabilidades.

- Valorar los principios éticos de la empresa, implica un impacto positivo cuando se asumen desde el eje rector que debe gobernar la seguridad de la información.

- Indicar a las empresas privadas y públicas la aplicación del documento CONPES.

- Concientizar por parte de empresas públicas y privadas con programas y/o campañas sobre ciberseguridad.

- Gestionar un departamento que se encargue de adoptar el proyecto donde se incluya la ciber conciencia.

8 BIBLIOGRAFÍA

ACURTIO DEL PINO, Santiago. [Sitio web]. Delitos Informáticos: Generalidades. [Consultado 10 de octubre 2021]. Disponible en: https://infolibros.org/pdfview/10122-delitos-informaticos-generalidades-dr-santiago-acurio-del-pino/

ALSINA RODRÍGUEZ, Juan Manuel. [Sitio web]. Recomendaciones para prevenir ciberataques. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2922/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

BYNUM, Ward. [Sitio web]. Alcances de una ética en el ciberespacio o el "giro" hacia una "ética floreciente". Citado por SIERRA GUTIÉRREZ, Luis Ignacio. Bogotá: 2009. Pontificia Universidad Javeriana.

BUSTAMANTE SANCHEZ, Ruben. [Sitio web]. Monografía. Universidad Autónoma del Estado de Hidalgo. [Consultado 14 octubre 2021]. Disponible en: https://infolibros.org/pdfview/10119-seguridad-en-redes-ruben-bustamante-sanchez/

CACERES GOYENECHE, Anderson David. [Sitio web]. Políticas de seguridad informática como herramienta para la preservación e integridad de la información en las empresas de seguridad privada en Bogotá. Tesis. Universidad Militar Nueva Granada, 2015. [Consultado 16 octubre 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7164/POLITICAS%20DE%20SEGURIDAD%20ensayo.pdf?sequence=1&isAllowed=y

CANDO-SEGOVIA, Mauricio Rodrigo. [Sitio web]. Prevención en ciberseguridad enfocada a los procesos de infraestructura tecnológica. [Consultado 16 octubre 2021]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7888164

CALETEC. Cómo evaluar el nivel de madurez en las empresas. [Sitio web]. [Consulta: 10 de abril 2022]. Disponible en: https://www.caletec.com/mejora-continua/como-evaluar-el-nivel-de-madurez-en-las-empresas/

CIBERSEGURIDAD LATAM. CONCIENTIZACIÓN. [Sitio web]. 44% de los usuarios sufrió un incidente de seguridad a través del correo electrónico. Disponible en: https://www.ciberseguridadlatam.com/2019/10/16/44-de-los-usuarios-sufrio-un-incidente-de-seguridad-a-traves-del-correo-electronico/

DELOITTE. [Sitio web]. ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía? [Consulta: 17 de octubre 2021]. Disponible en:

https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Informe-WannaCry.pdf

DUQUE B, Jhon F; SILVA, Larry Andres y RENTERÍA, Daliza. [Sitio web]. 2008. Análisis comparativo de las principales técnicas de hacking empresarial. [Consultado 10 de octubre 2021]. Disponible en: https://infolibros.org/pdfview/5061-analisis-comparativo-de-las-principales-tecnicas-de-hacking-empresarial-articulo-jhon-f-duque-b-larry-andres-silva-y-edys-daliza-renteria/

EL TIEMPO. [Sitio web]. Bogotá: EL TIEMPO, Conciencia de seguridad informática. [Consulta: 10 de octubre 2021]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-885611

EMAVITIC. [Sitio web]. Congreso Internacional en Tecnologías de la Información y Ciberseguridad 2016. [Consulta: 10 de octubre 2021]. Disponible en: https://catalogoenlinea.bibliotecanacional.gov.co/client/es_ES/search/asset/138310/0

EFE. [Sitio web]. Los ciberataques en Latinoamérica han aumentado un 24 % este año. [Consulta: 11 de octubre 2021]. Disponible en: https://www.efe.com/efe/america/tecnologia/los-ciberataques-en-latinoamerica-han-aumentado-un-24-este-ano/20000036-4619548

FERNÁNDEZ, Luis Jonalber. [Sitio web]. Incidencia del factor humano en la seguridad de la información de las organizaciones públicas de categoría 6. [Consulta: 11 octubre 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/38893/ljfernandez.pdf?sequence=3&isAllowed=y

FORBES CENTRO AMERICA. [Sitio Web]. Forbes Staff. 2020. La ciberseguridad antes, durante y después de la pandemia. [Consulta: 11 octubre 2021]. Disponible en: https://forbescentroamerica.com/2020/07/14/la-ciberseguridad-antes-durante-y-despues-de-la-pandemia/

FORD, Ealine y WECK, Winfried. [Sitio web]. Internet y pandemia en las Américas. [Consulta: 18, septiembre 2021]. Disponible en: https://www.kas.de/documents/7851262/8887001/LIBRO+INTERNET+Y+PANDEMIA+EN+LAS+AMERICAS+VF.pdf/4a2051a3-c28a-f978-1343-5a9e4168d6ee?version=1.0&t=1608242281728

GARCÍA FORERO, Luis Felipe Guillermo. [Sitio web]. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2c%20el%20personal.pdf?sequence=1&isAllowed=y

GB-ADVISORS. [Sitio web] ¿Por qué medir el nivel de madurez de los procesos en tu empresa?. [Consulta: 10 de abril 2022]. Disponible en: https://www.gb-advisors.com/es/medir-nivel-de-madurez-procesos-empresa/

GIBSON, William. [Sitio web]. Neuromante. Estados Unidos. [Consulta: 29 septiembre 2021]. Disponible en: https://lamanodelextranjero.com/2017/04/27/neuromante-quien-es-quien-en-el-ciberespacio/

GONZÁLEZ HERNÁNDEZ, Edwin Mauricio [Sitio web]. Actualidad de Colombia en seguridad de la información. [Consulta: 14 de octubre 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2882/Trabajo%20de%20grado1886.pdf?sequence=1&isAllowed=y

GONZÁLEZ DÍAZ, David Leonardo. [Sitio web]. La ciberseguridad política clave dentro de las organizaciones. [Consulta: 14 de octubre 2021]. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/37635/2021davidgonzalezsaulpulido.pdf?sequence=1&isAllowed=y

GUERRERO VALLEJO, Gina Yuleisi. [Sitio web]. Operaciones cibernéticas y seguridad hemisférica en Colombia: análisis desde la cooperación regional e internacional. [Consulta: 14 de octubre 2021]. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/42878/2022ginaguerrero.pdf?sequence=1&isAllowed=y

INCIBE. [Sitio web]. Ciberseguridad en el teletrabajo. [Consulta: 14 de octubre 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

INCIBE. [Sitio web]. Comparativa de empresas sobre la concienciación en ciberseguridad. [Consulta: 14 de octubre 2021]. Disponible en: https://www.youtube.com/watch?v=Y6vO2HxrEPc

INFOLIBROS. [Sitio web]. POLITICAS DE SEGURIDAD INFORMÁTICA (PSI), Departamento de Tecnología Organización Inca. [Consulta: 16 de octubre 2021]. Disponible en: https://infolibros.org/pdfview/10132-politicas-de-seguridad-informatica-psi-organizacion-inca/

INTER-AMERICAN DEVELOPMENT BANK. [Sitio web]. Ciberseguridad. Riesgos, avances y el camino a seguir en américa latina y el caribe. 2020. [Consultado 10 septiembre 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-

Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

INTEREMPRESAS. [Sitio web]. Construir un firewall humano para hacer frente a las amenazas internas. [Consulta: 15 de octubre 2021]. Disponible en: https://www.interempresas.net/Ciberseguridad/Articulos/315950-Construir-un-firewall-humano-para-hacer-frente-a-las-amenazas-internas.html

IPMOGUIDE. [Sitio web]. Modelo de Madurez. [Consulta: 02 de abril 2022]. Disponible en: https://ipmoguide.com/cobit-modelo-de-madurez/

INSOLTEC. [Sitio web]. Niveles De Madurez En Transformación Digital De Las Organizaciones En Chile. [Consulta: 04 de abril 2022]. Disponible en: https://www.insoltec.cl/niveles-de-madurez-en-transformacion-digital-de-las-organizaciones-en-chile/

ISO. [Sitio web]. Sistemas de gestión de la calidad. [Consulta: 25 septiembre 2021]. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:9001:ed-4:v2:cor:1:v1:es

ISOTOOLS. [Sitio web]. ISO 27002. [Consulta: 05 de abril 2022]. Disponible en: https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/#:~:text=El%20objetivo%20que%20persigue%20la,de%20la%20administraci%C3%B3n%20de%20riesgos

KASPERSKY. [Sitio web]. Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [Consulta: 20 septiembre 2021]. Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

KYMATIO. [Sitio web]. El INCIBE británico (NCSC): «Las personas pueden ser el eslabón más fuerte en ciberseguridad. [Consulta: 20 febrero 2022]. Disponible en: https://blog.kymatio.com/es/el-incibe-britanico-ncsc-las-personas-pueden-ser-el-eslabon-mas-fuerte-en-ciberseguridad/

MICROSOFT. [Sitio web]. News Center Microsoft Latinoamérica, La ONU logra avances importantes en ciberseguridad. [Consulta: 02 de octubre 2021]. Disponible en: https://news.microsoft.com/es-xl/la-onu-logra-avances-importantes-en-ciberseguridad/

MINISTARIO DE DEFENSA. [Sitio web]. Ciberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio. 2010. [Consultado 15 de octubre de 2021]. Disponible en: https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

MINISTERIO DE DEFENSA. [Sitio web]. Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario. España: Centro Superior de Estudios de la Defensa Nacional. Escuela de altos estudios de la defensa. 2012. 337p. [Consulta: 10 de abril 2022]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_ceseden_137.pdf

MINTIC. G.ES.05. [Sitio web]. Diseño e implementación de una estrategia de seguridad de la información. [Consulta: 10 de abril 2022]. Disponible en: https://www.mintic.gov.co/arquitecturati/630/articles-9483_recurso_pdf.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. [Sitio web]. Recomendaciones sobre Ciberseguridad Teletrabajo. [Consulta: 16 de octubre 2021]. Disponible en: https://teletrabajo.gov.co/622/w3-article-126328.html

NACIONES UNIDAS. [Sitio web]. Ciberseguridad. [Consulta: 08 de octubre 2021]. Disponible en: https://www.un.org/counterterrorism/es/cybersecurity

NACIONES UNIDAS. [Sitio web]. Examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo. [Consulta: 11 de octubre 2021]. Disponible en: https://undocs.org/es/A/RES/72/284

NOVA ALARCÓN, Michael Alejandro. [Sitio web]. Ciber estrategia Colombia. [Consulta: 11 de octubre 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/14171/MichaelAlejandroNovaAlarcon2016.pdf?sequence=1&isAllowed=y

LA REPÚBLICA. [Sitio web]. BANCOS / Las nuevas modalidades de vishing, smishing y fishing con las que hacen fraude bancario. [Consulta: 11 de octubre 2021]. Disponible en: https://www.larepublica.co/finanzas-personales/las-nuevas-modalidades-de vishing-smishing-y-fishing-con-las-que-hacen-fraude-bancario-2969016

OSPINA DÍAZ, Milton Ricardo. [Sitio web]. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*. [Consulta: 11 de octubre 2021]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7667839

OSPINA DIAZ, Milton Ricardo y SANABRIA RANGEL, Pedro Emilio. [Sitio web]. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Bogotá (Colombia). 26 noviembre 2020. vol.62 no.2. [Consultado 01 octubre 2021]. ISSN 1794-3108. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199#fn4

ORGANIZACIÓN DE ESTADOS AMERICANOS. [Sitio web]. El derecho internacional y las operaciones cibernéticas de los estados: mejorar la transparencia. [Consulta: 6 octubre 2021]. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI_doc_578-19.pdf

PARRA, Carlos Humberto. [Sitio web]. Seguridad informática y seguridad de la información en el mundo, como factor de enseñanza en Colombia. [Consulta: 6 octubre 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2856/00002352.pdf?sequence=1

PERALTA CUADRADO, Mary Luz Roa Ibarra. [Sitio web]. El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia. [Consulta: 6 octubre 2021]. Disponible en: https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/3949/EL%20IMPACTO%20DEL%20DELITO%20CIBERN%c3%89TICO%20EN%20LAS%20OPERACIONES%20DE%20COMERCIO%20ELECTR%c3%93NICO%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

PÉREZ PÉREZ, Yuly. [Sitio web]. Importancia de la ciberseguridad en Colombia. [Consulta: 6 octubre 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

POLICIA NACIONAL, DIJIN, CCIT, TICTAC, SAFE. [Sitio web]. TENDENCIAS CIBERCRIMEN COLOMBIA 2019 – 2020. [Consulta: 6 octubre 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

REVISTA OBSERVACIONES FILOSÓFICAS. [Sitio web]. Notas sobre el estado ético de la tecnología génica. El hombre operable. Conferencia: 19 de mayo 2000, Centro de Estudios Europeos (CES) Universidad de Harvard, EE UU. [Consulta: 6 octubre 2021]. Disponible en: https://www.observacionesfilosoficas.net/elhombreoperable.html

RIVEROS CARDENAS, Fredy Orlando. [Sitio web]. Administración del riesgo cibernético un enfoque desde la alta gerencia empresarial en Colombia. [Consulta: 6 octubre 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/15837/RiverosCardenasFredyOrlando2017.pdf?sequence=1&isAllowed=y

ROMERO CASTRO, Martha Irene. [Sitio web]. Introducción a la seguridad informática y el análisis de vulnerabilidades. [Consultado 10 octubre 2021]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

SANCHEZ MONTAÑES, Carmen. Literario [Sitio web]. Tesis doctoral. Universidad de Sevilla. 2020 [Consultado 10 octubre 2021]. Disponible en: https://idus.us.es/bitstream/handle/11441/63996/COPIA%20TESIS.pdf?sequence=1&isAllowed=y

SEMANA. [Sitio web]. Bogotá: SEMANA. El año de los ciberataques en Colombia, estas son las alarmantes cifras. [Consulta: 07 de octubre 2021]. Disponible en: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

SCIELO. [Sitio web]. Modelos de Madurez en los Datos de una Organización; Caso de Estudio. [Consulta: 01 de abril 2022]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892012000200004

SIERRA GUTIÉRREZ, Luis Ignacio. [Sitio web]. Alcances de una ética en el ciberespacio o el "giro" hacia una "ética floreciente". Bogotá 2009. Pontificia Universidad Javeriana. [Consulta: 01 de abril 2022]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232009000200006

SISTEMA UNICO DE INFORMACIÓN NORMATIVA. [Sitio web]. Ley 1928 de 2018 “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest. [Consulta: 12 octubre 2021]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501

SOFTTEK. [Sitio web]. El 27% de ciberataques están ocasionados por empleados. [Consulta: 15 de octubre 2021]. Disponible en: https://softtek.eu/tech-magazine/cybersecurity/el-27-de-los-ciberataques-estan-ocasionados-por-el-personal-de-la-empresa/

SOFISTIC, CIBERSECURITY. [Sitio web]. 2020. En la actualidad, el mayor reto es la inteligencia artificial ofensiva. [Consulta: 10 octubre 2021]. Disponible en: https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

SEGURIDAD INTERNACIONAL. [Sitio web]. 2015. aspectos legales en el ciberespacio. la ciberguerra y el derecho internacional humanitario. [Consulta 14 octubre 2021]. Disponible en: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

SOPHOS. [Sitio web]. Informe de amenazas 2021 de SOPHOS. [Consulta: 10 de octubre 2021]. Disponible en: https://www.sophos.com/es-es/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

SORIA GUZMAN, Irene. Ética hacker, seguridad y vigilancia. [Sitio web]. 2016, noviembre. [Consultado 10 de octubre 2021]. Disponible en: https://infolibros.org/pdfview/5054-etica-hacker-seguridad-y-vigilancia-universidad-del-claustro-de-sor-juana/

SORIA OLIVAS Emilio; TORRES, José; PADIAL, Óscar y otros. [Sitio web]. Ciberseguridad. El reto del siglo XXI. Parc Cientific (España): Universidad de Valencia. 2019. [Consultado 14 octubre 2021]. Disponible en: https://invaci.es/wp-content/uploads/2021/08/CIBERSEGURIDAD-EL-RETO-DEL-SIGLO-XXI.pdf

TEH MISSING REPORT. [Sitio web]. 30 estadísticas de Seguridad Informática que Importan (Actualizadas al 2021). [Consulta: 05 de octubre 2021]. Disponible en: https://preyproject.com/blog/es/30-estadisticas-seguridad-informatica/

TEH MISSING REPORT. [Sitio web]. Phishing en Latinoamérica: El panorama 2020.[Consulta: 05 de octubre 2021]. Disponible en: https://preyproject.com/blog/es/phishing-en-latinoamerica-el-panorama-2020/

TORRES SOLER, Luis Carlos. [Sitio web]. La complejidad humana. [Consultado 13 de octubre 2021]. Disponible en: https://disi.unal.edu.co/~lctorress/tgs/Tgs003.pdf

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA. [Sitio web]. El principio de reconocimiento mutuo como fundamento de la cooperación judicial penal y sus efectos en los ordenamientos de los estados miembros. [Consulta: 5 octubre 2021]. Disponible en: http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:19800&dsID=PriRecMut.pdf

UNIVERSIDAD ORT DE URUGUAY. [Sitio web]. Uruguay. Facultad de Ingeniería, La conciencia en el uso de herramientas informáticas es fundamental para evitar ataques. [Consulta: 01 de octubre de 2021]. Disponible en: https://fi.ort.edu.uy/8978/33/la-conciencia-en-el-uso-de-herramientas-informaticas-es-fundamental-para-evitar-ataques.html

UPCOMMONS. Resumen de los Modelos Kaizen, Lean y Six Sigma. [Sitio web]. [Consulta: 02 de abril 2022]. Disponible en: https://upcommons.upc.edu/bitstream/handle/2099.1/10317/A.4.%20Resumen%20de%20los%20modelos%20Kaizen,%20Lean%20y%20Six%20Sigma.pdf?sequence=5

VARGAS SALCEDO, Julio Cesar. [Sitio web]. Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para

la mitigación del riesgo sobre los datos de la empresa. Fundación Universidad Piloto de Colombia. [Consultado 12 octubre 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00004663.pdf

VODAFONE. [Sitio web]. Consejos para mejorar tu teletrabajo. [Consulta: 13 de octubre 2021]. Disponible en: https://ideasparatuempresa.vodafone.es/wp-content/uploads/2020/04/EBOOK-TELETRABAJO-IDEAS-PARA-TU-EMPRESA.pdf

ZAMBRANO GRANADA, Dayhann Geraldynn (2019). [Sitio web]. La falta de conciencia, una vulnerabilidad latente para la seguridad de la información. [Consulta: 13 de octubre 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2922/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y