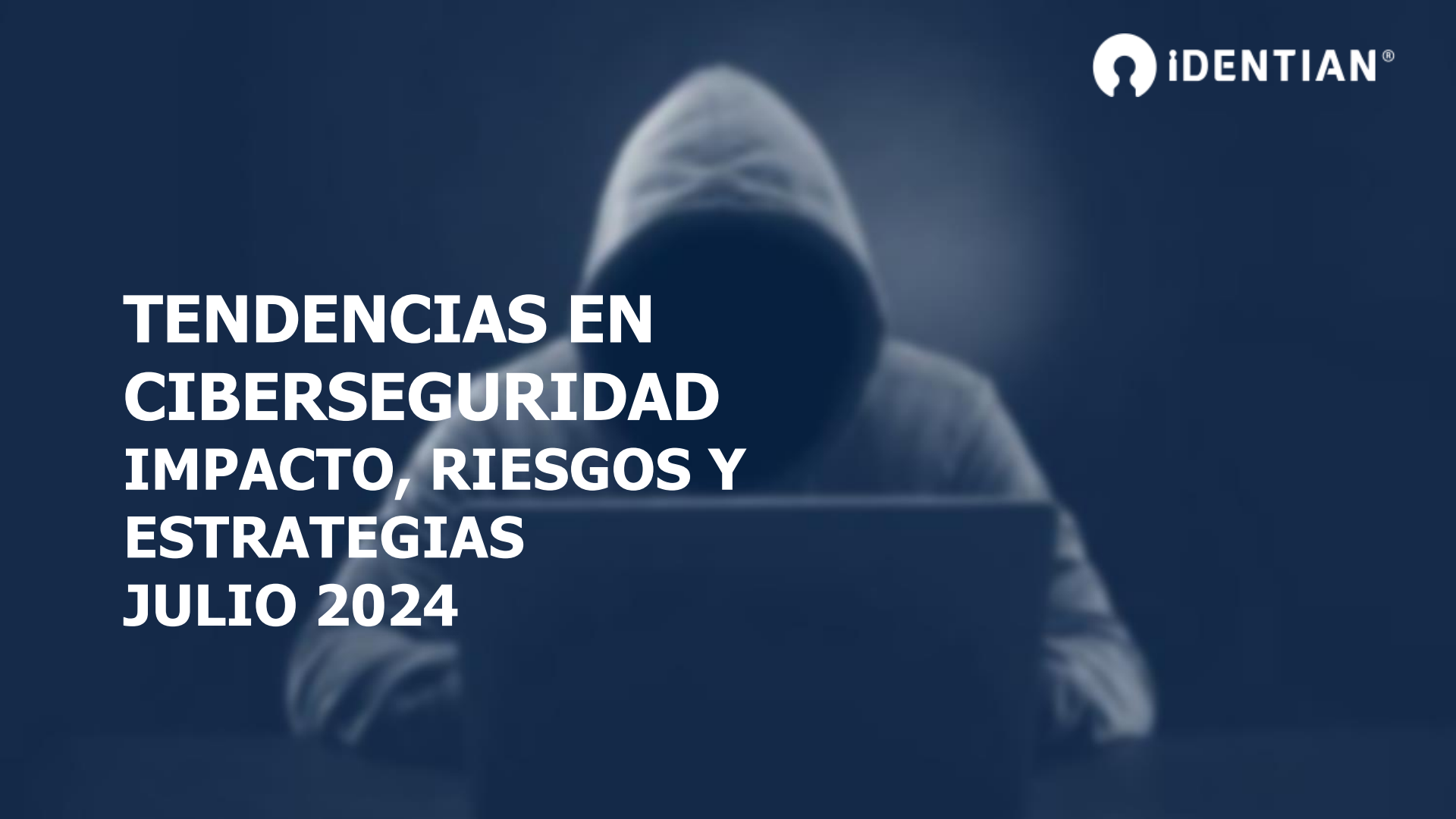


TENDENCIAS EN CIBERSEGURIDAD

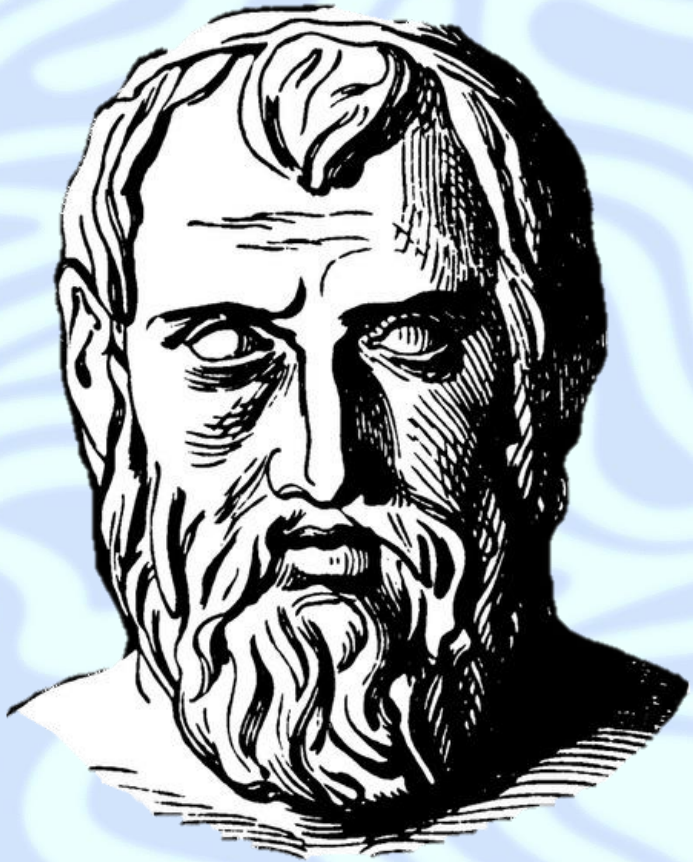
IMPACTO, RIESGOS Y ESTRATEGIAS

JULIO 2024


IDENTIAN®
PROPOSITO
SUPERIOR

"La desconfianza es la madre de la seguridad".

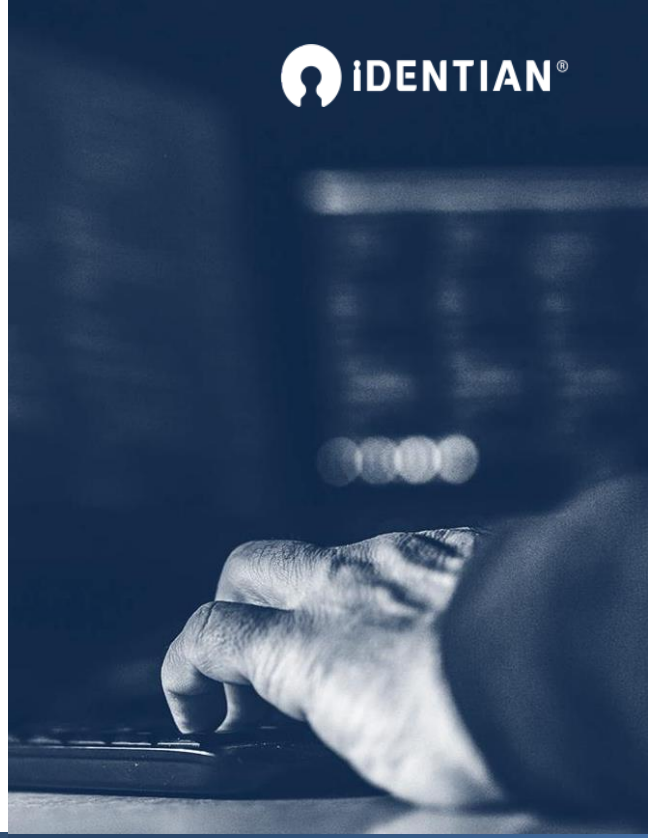
Aristófanes



IDENTIAN®

AGENDA PRESENTATION

1. Familia IDENTIAN
2. Fallo Mundial Tecnológico – Caso CrowdStrike 2024
3. Tendencias de CIberseguridad en Colombia – Ransonware
4. Seres Humanos Pilares de Ciberseguridad
5. Riesgos vs IA/Machine Learning/ Bigdata
6. Hackers, desmitifiquemos el misterio
7. Estrategias de ciberseguridad
8. Conclusiones y Recomendaciones



1. Familia IDENTIAN

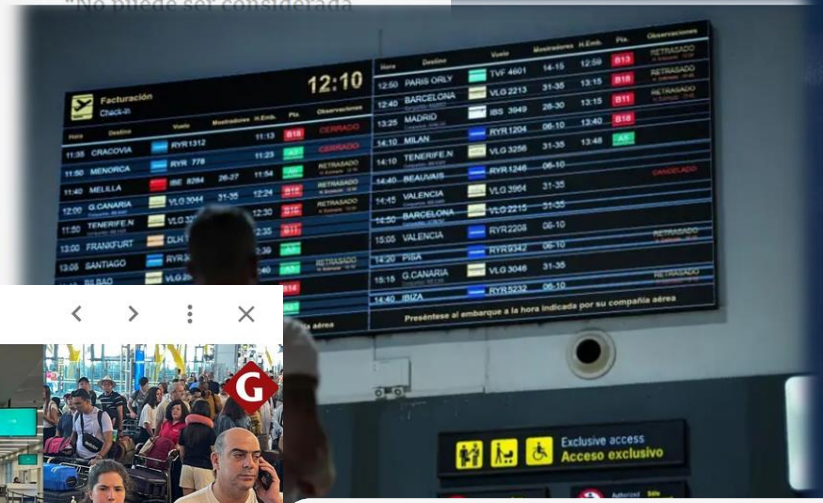
2. CASO CROWDSTRIKE

IDENTIAN®

Qué es Crowdstrike, la empresa de ciberseguridad responsable del apagón informático global

Principales noticias

"No puede ser considerada



https://www.youtube.com/watch?v=IcSMZ-pI8bw

3. TENDENCIAS DE CIBERSEGURIDAD EN COLOMBIA

El cibercrimen

"No es cuestión de estratos"

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO

Según cifras del Cybersecurity Ventures sobre economía cibernética global, el costo del cibercrimen alcanzará en 2025 los **10.5 billones de dólares**; lo que equivale a la suma de las economías de Japón, tercera en el planeta, Alemania cuarta y Suiza la 18ª; se estima entonces que durante el 2022 los costos por daños globales del cibercrimen estarán alrededor de **6 trillones de dólares**, lo que equivale a 648 millones de dólares en pérdidas por hora; 11.4 millones de dólares en un minuto y cerca de 190.000 dólares por segundo.

De acuerdo con el **Foro Económico Mundial** y la ONU, el **cibercrimen** solo está por debajo de los desastres naturales y el cambio climático como uno de los principales riesgos para la humanidad.

IDENTIAN®

CIFRAS

1.9 millones

Impacto promedio a una organización en américa latina

-Multas
-Impacto reputacional
-Demandas

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO

Principales riesgos "Geopolíticos" hasta 2025

1	Del mundo unipolaí a un mundo más multipolaí que nunca
2	Empíesas, los nuevos pesos pesados de la geopolítica
3	De la gueíía convencional a la gueíía híbíida
4	La infoímación es podeí, peío el BIG DAI'A es podeí exponencial
5	Un nuevo mundo de íiesgos y amenazas específicos
6	A las pueítas de la píóxima gían cíisis económica
7	Noímalización del conflicto (y de la violencia)
8	Aumento de los casos de "Bíexit" ante las cíisis de lideíazgo
9	Polaíización ideológica en Latinoaméíica
10	Consolidación de las gueíías peípetuas en Oíiente Medio

Fuente: LISA INSTITUTE

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO

Principales riesgos "Geopolíticos" hasta 2025

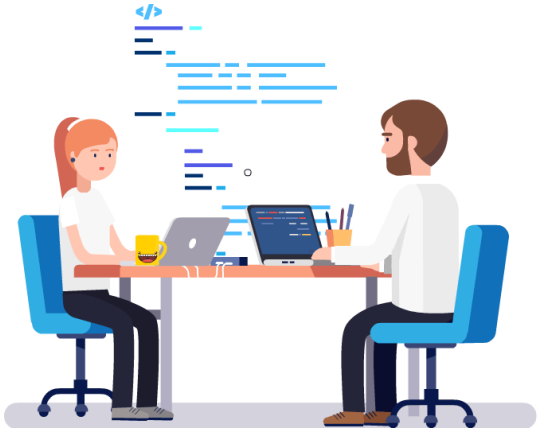
Fuente: LISA INSTITUTE

IDENTIAN®

ACTUALIDAD DEL DELITO INFORMATICO

Trabajar desde casa, además, puede dar una falsa sensación de seguridad y abre la puerta a mostrarse confiado ante enlaces o documentos adjuntos de procedencia sospechosa. La presa más fácil para los hackers, sin embargo, son las **personas**, por lo general mayores o no técnicas, que están poco acostumbradas a usar internet como lugar de trabajo y se ven forzadas a entrar estos días para estar dentro de la "Nueva normalidad".

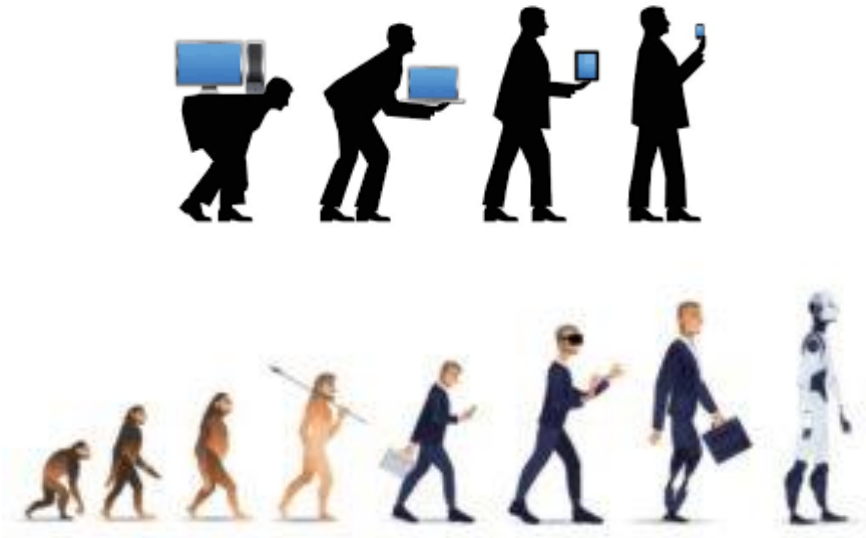
Fuente: ABC REDES



- **Fraudes online aumentan, "el miedo es el señuelo" "FEARWARE"**
- **Ataques se concentran en el sector salud, infraestructuras críticas, banca**
- **El teletrabajo sin planificación ni control es una brecha permanente**

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO



La evolución de la ciberseguridad es directamente proporcional a los avances en las tecnologías de la información y las telecomunicaciones, de igual forma lo han hecho los ciberataques y su sofisticación y aunque el lado del bien trata de hacer su mejor esfuerzo, el **lado oscuro** ha sido sin duda el alumno aventajado hasta ahora.

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO

80´s

Gusano Morris se convierte en el primer gusano de red, nacen los primeros malwares y entra en auge la industria de antivirus

90´s

Llega el auge de internet como lo conocemos, se crear el primer firewall de inspección y los medios extraíbles crean nuevos vectores de ataque.

2000

Auge del e-mail e ingeniería social. Vulnerabilidades informáticas sobrepasan la capacidad de los sistemas de protección. Cae Estonia - Iloveyou - Conficker

2010

Ciberataques con nivel de sofisticación sin precedentes Cibercrimen organizado, malware se vuelve indetectable. Móviles como vector principal. Stuxnet

2020

Ciberataques de nivel militar, auge del DDoS. Capacidad de propagación de malware exponencial. WannaCry - NotPetya

IDENTIAN®

EVOLUCION DEL DELITO INFORMATICO

Ransomware Timeline

1989

First known ransomware attack. Biology researcher sends 5.5" floppies purporting to have AIDS research on it to thousands of interested parties. "AIDS Trojan" encrypts files and file names, demands payment to unencrypt. Solution quickly found; idea takes hold years later in larger criminal community.

2000s

Ransomware trojans develop. "Blockers" interfere with normal computer functions demanding ransom for removal. Removable by sophisticated users.

2010

Ransomware becomes more dangerous. "Cryptors" convert data to encrypted code, for which only criminals hold the decryption key. Criminals combine blockers with cryptors, doubling the avenues for demanding payment.

2015

Ransomware moves almost exclusively to encryption of files. Criminals demand payment in cryptocurrency which has anonymization features that make tracking harder.

2017 - Present

Attacks and demands skyrocket. While continuing to attack individuals and small businesses, criminals begin going after bigger targets, including municipal organizations, governments, and companies across the spectrum. The 2017 WannaCry ransomware infects over 500,000 computers devices across the globe, and causes $4 billion in damage. The damage from NotPetya ransomware exceeds $10B. Ransomware attacks continue to evolve.

Kaseya

JBS

Colonial Pipeline Company

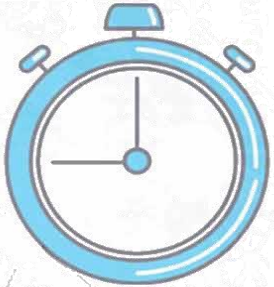
Cnt

Fuente: ACA GROUP

EVOLUCION DEL DELITO INFORMATICO

Global Ransomware Damage Costs*

- **2015: $325 Million**
- **2017: $5 Billion**
- **2021: $20 Billion**
- **2024: $42 Billion**
- **2026: $71.5 Billion**
- **2028: $157 Billion**
- **2031: $265 Billion**



Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

CYBERSECURITY VENTURES

* SOURCE: CYBERSECURITY VENTURES

IDENTIAN®

EL IMPACTO DEL RANSOMWARE EN COLOMBIA

El ransomware ha tenido un impacto significativo en Colombia, afectando a empresas de todos los tamaños, hospitales y usuarios individuales.

El estudio ‘The State of Ransomware 2023’ publicado por la firma de seguridad informática Sophos, el pasado 11 de mayo, reveló que el ritmo de los ataques de ransomware se ha mantenido constante, con un 66 % de los encuestados informando que su organización fue atacada por ransomware en el último año.

ESTADÍSTICAS Y CASOS DESTACADOS

400%
Aumento en los ataques de ransomware en Colombia en los últimos 2 años.

Hospital XYZ

Ransomware bloqueó el acceso a los registros médicos de miles de pacientes, poniendo en riesgo su atención médica.

Empresa ABC
Pagó un rescate de $100,000 para recuperar el acceso a sus datos críticos, pero no se garantizó la recuperación completa.

ESTADÍSTICAS Y CASOS DESTACADOS

Año	Porcentaje de organizaciones atacadas	Número de encuestados
2020	51 %	5,000
2021	37 %	5,400
2022	66 %	5,600
2023	66 %	3,000

CAUSAS PRINCIPALES DE LOS ATAQUES DE RANSOMWARE EN 2023

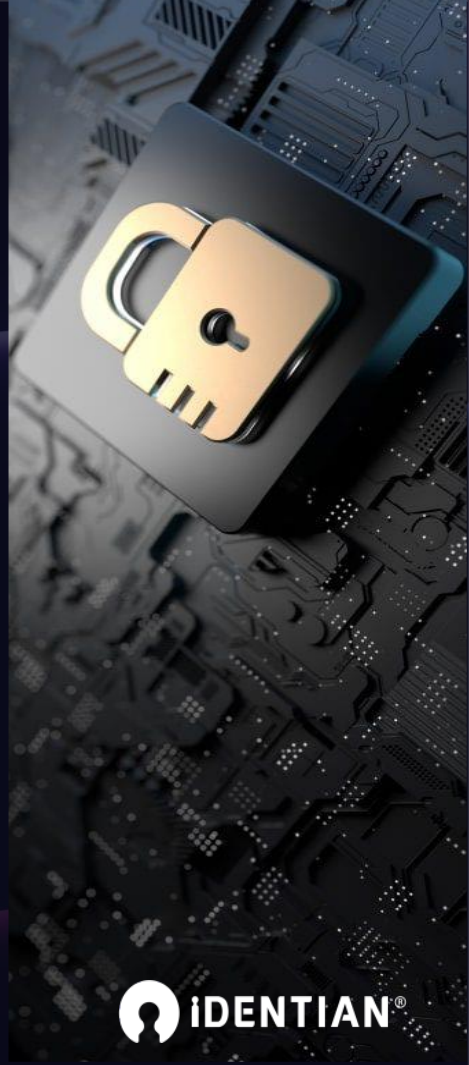
Causa	Porcentaje
Vulnerabilidad	36 %
Credenciales comprometidas	29 %
Correo electrónico malicioso	18 %
Phishing	13 %
Ataque de fuerza bruta	3 %
Descarga	1 %

¿EN CUÁNTOS ATAQUES LLEGAN A CIFRAR LOS DATOS?

Los ciberdelincuentes están logrando cifrar datos de sus víctimas en más de tres cuartas partes (76 %) de los ataques de ransomware. De hecho, los niveles de cifrado están ahora en su punto más alto en los últimos cuatro años. Esto probablemente refleja el nivel de habilidad cada vez mayor de los adversarios que continúan innovando y refinando sus enfoques.

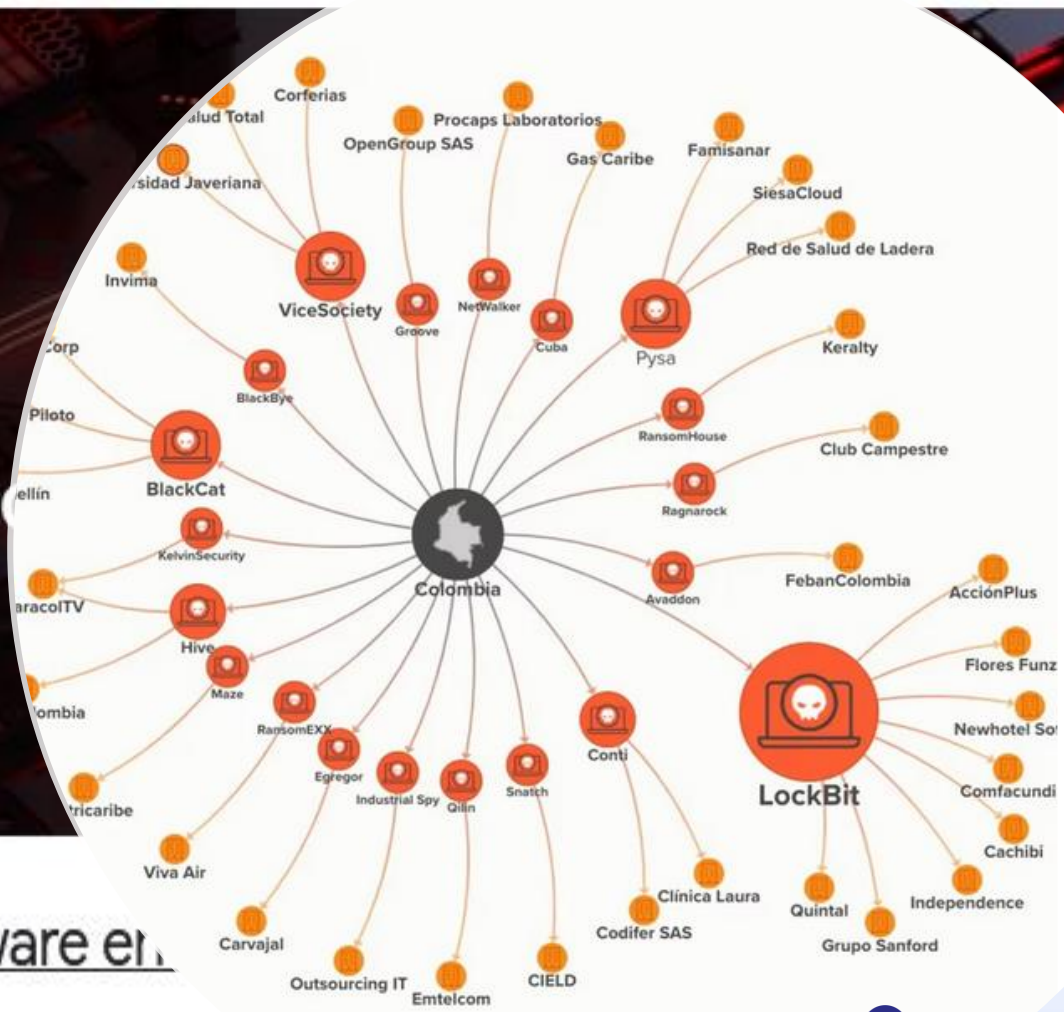
TASA DE CIFRADO DE DATOS EN ATAQUES DE RANSOMWARE (2020-2023)

Año	Datos cifrados	Ataque detenido antes del cifrado	Extorsión sin cifrado
2020	65 %	31 %	4 %
2021	54 %	21 %	7 %
2022	73 %	24 %	3 %
2023	76 %	3 %	3 %



ManageEngine

2022 fue el año del ransomware en Col



2022 fue el año del ransomware en
ManageEngine Blog

IDENTIAN®

LA NOTA ECONÓMICA

Colombia recibió 20 mil millones de intentos de ciberataques en 2022, un crecimiento del 80% frente a 2021.

marzo 2, 2023

EL TIEMPO

Colombia, el segundo país de América Latina con más ciberataques en 2022

01 de marzo 2023,

infobae

Nutresa fue objeto de un
compañía confirmó que
ransomware

21 Abr, 2023

LR

PROGRAMA: INSIDE LR | TECNOLOGÍA

Audifarma sufrió at
se suma a otras emp
víctimas

lunes, 23 de enero de 2023

BBC NEWS | MUNDO

Noticias América Latina Internacional Coronavirus Hay Festival Economía Ciencia Salud Cultura Tecnología Video Centroamérica Cuenta

"Los hackers nos aventajan porque hay poca gente especializada en ciberseguridad. No damos abasto": Soledad Antelada, la latina que protege al Departamento de Energía de EE.UU.

José Carlos Cueto
BBC News Mundo

infobae

ontra Sanitas causa viacrucis de

cibernético a sistema de la
ana

infobae

COLOMBIA

Ataque cibernético a página web del Invima tiene en vilo información y aplicativos internos del instituto

El ataque se produjo en la madrugada de este lunes y por ahora el portal www.invima.gov.co está deshabilitado

4 de Octubre de 2022

will result in
human casualties

2025

Gartner

n: EPM anuncia ataque de
ciberseguridad a su sistema

IDENTIAN®

COLOMBIA EN CIBERIESGO?

- Sistema de suministro eléctrico
- Servicios gubernamentales y judiciales
- Sistema sanitario
- Sistema educativo
- Telecomunicaciones & BPO
- Gas & Oil
- Sistemas de suministro de alimentos (producción, almacenamiento y distribución)

epm
afinia Grupo epm
Electricaribe
EMCALI
FISCALÍA GENERAL DE LA NACION
PRESIDENCIA DE LA REPÚBLICA
invima Instituto Nacional de Vigilancia de Medicamentos y Alimentos
SUPERINTENDENCIA DE SOCIEDADES
PROCAPS
Sanitas
AUDIFARMA
SaludTotal EPS-S
Famisanar EPS
Pontificia Universidad JAVERIANA Colombia
U2 Universidad Piloto de Colombia
UNIVERSIDAD EL BOSQUE
PRISA RADIO
corferias Generadores de Oportunidades y Progreso
CARACOL TELEVISIÓN
ACCIONPLUS TALENTO INTEGRAL
OUTIT
ifx Networks
Quintal
Independence
Gases del Caribe
IDENTIAN
Grupo nutresa

COLOMBIA EN CIBERIESGO?

Servicios gubernamentales y judiciales

FISCALÍA GENERAL DE LA NACION

PRESIDENCIA DE LA REPÚBLICA

invima
Instituto Nacional de Vigilancia de Medicamentos y Alimentos.

SUPERINTENDENCIA DE SOCIEDADES

ifx Networks

Salud

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Rama Judicial
República de Colombia

Industria y Comercio
SUPERINTENDENCIA

Industria y Comercio
SUPERINTENDENCIA

Coljuegos

IDENTIAN®

Los desafíos de un ciberataque en el sector del transporte

Publicado: 07 Marzo 2024

Desde algunos meses se conocen las cifras económicas del sector del transporte después de la crisis del Covid, y lo que se puede decir es que el sector del transporte ha repuntado bien tanto en Francia como en el extranjero.

Al igual que todos los otros sectores de la economía, el transporte está experimentando una digitalización masiva en todo el mundo. Esta oportunidad de crear valor mediante la modernización también representa una oportunidad para los piratas informáticos que tienen cada vez más posibilidades para atacar los sistemas y empresas de transporte (desde el transporte de personas hasta la logística industrial).

¿A qué tipos de ataques informáticos las infraestructuras del transporte deben enfrentarse? ¿Cómo pueden prepararse? He aquí unos consejos para limitar los riesgos de ciberataques en el sector del transporte.

Numerosos y edificantes ataques

Existen varios tipos de ciberataques en el sector del transporte. Según el informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), las principales amenazas para el sector del transporte son:

- Los ataques por ransomware
- Las amenazas vinculadas al robo y la compromisión de datos
- Malware
- los ataques de tipo DDoS (Distributed Denial-of-Service)
- El phishing
- Los ataques a la cadena de suministro

IDENTIAN®

4. SERES HUMANOS PILARES DE CIBERSEGURIDAD

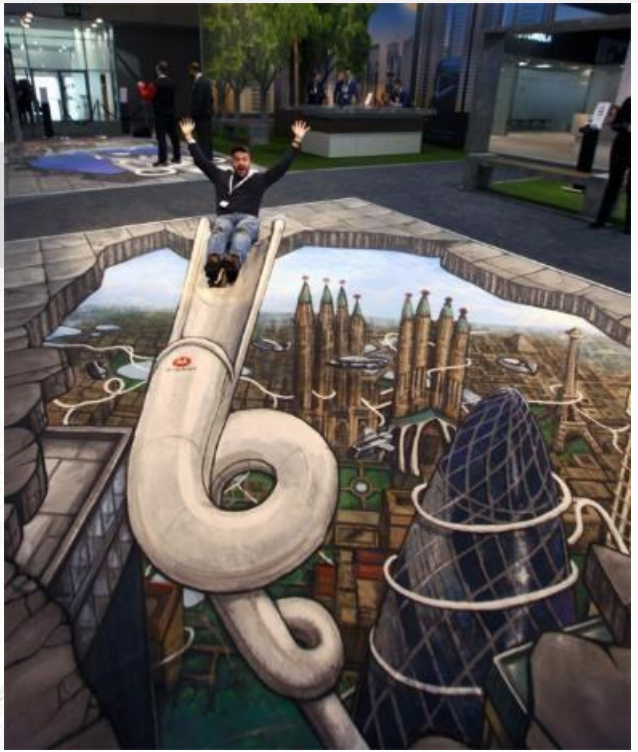

La ingeniería social es una de las formas en las que los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. Ya que la ingeniería social se basa en la naturaleza humana y las reacciones humanas, hay muchas formas en que los atacantes pueden engañar, en línea o sin conexión.
CIBERCRIMEN E
INGENIERÍA SOCIAL
IDENTIAN®

INGENIERIA SOCIAL

El papel del engaño?

El propósito del engaño es crear una ***ilusión***, la cual de algún modo beneficia a nuestro "**ingeniero social**".

El engaño es básicamente la manipulación de información o una situación para producir una realidad deseada.



IDENTIAN®

INGENIERIA SOCIAL

¿Por qué utilizar Ingeniería Social?

Podemos responderlo con dos frases:

» Porque no existe parche para la interfaz humana.

» Las personas son la vulnerabilidad más grande en cualquier red.

INGENIERIA SOCIAL

Hackers

Espías Industriales / Agentes de Espionaje Industrial

Gobiernos Extranjeros / Agentes del Gobierno

Extranjeros

Ladrones de Identidad.

Empleados enojados..

Recolectores de Inteligencia Empresarial.

Agentes de Información Investigadores Privados.

IDENTIAN®

TIPOS DE INGENIERIA SOCIAL

Tecnológico

Consiste en hacerle creer a la persona que esta interactuando realmente con un programa u ordenador con el fin de que nos provea información valiosa

Humano

Utilizar la naturaleza humana de ser util, eficiente o caer bien a travez de una persona con autoridad.

IDENTIAN®

PHISHING, FRAUDE, RIESGOS

CONSISTE EN EL ROBO DE INFORMACIÓN PERSONAL O FINANCIERA, A TRAVÉS DE LA FALSIFICACIÓN DE UN SITIO OFICIAL, DE ESTA FORMA EL USUARIO CREE INGRESAR SUS DATOS EN UN LUGAR CONFIABLE, PERO EN REALIDAD SON ENVIADOS A UN DELINCUENTE

FALSIFICACIÓN DE UN SITIO OFICIAL

ENVÍO DE MSJ POR ALGUN MEDIO DE PROPAGACIÓN

UN %DE USUARIOS CONFÍA Y HACE CLICK EN EL ENLACE (SEÑUELO)

EL USUARIO INGRESA AL SITIO FALSO Y DEJA SU INFORMACIÓN

EN OCASIONES SE SOLICITA DESCARGAR ARCHIVOS

EL DELINCUENTE OBTIENE LA INFORMACIÓN Y LE DA EL USO FINAL

MEDIOS DE PROPAGACIÓN

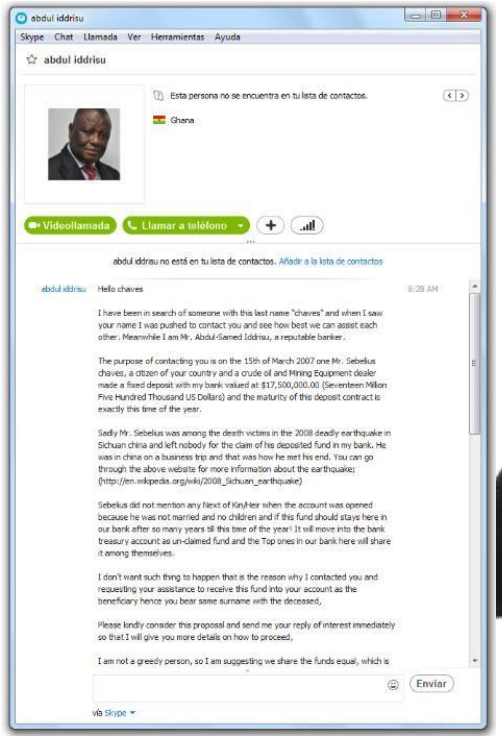
CORREO ELECTRÓNICO
REDES SOCIALES
SMS/WHATSAPP
LLAMADAS TELEFÓNICAS
PAGINAS WEB

IDENTIAN®

PHISHING, FRAUDE, RIESGOS

ALGUNAS VARIANTES

VISHING



ESTAFA NIGERIANA

SMISHING

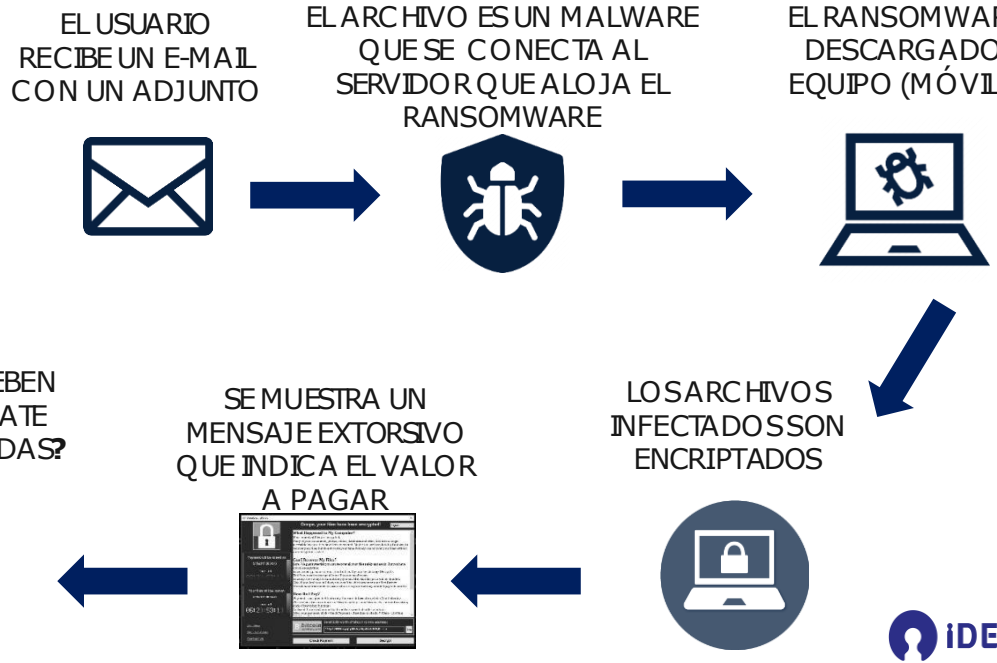
SPEAR PHISHING

iDENTIAN®

PHISHING, FRAUDE, RIESGOS

RANSOMWARE

*El **ransomware** es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña*

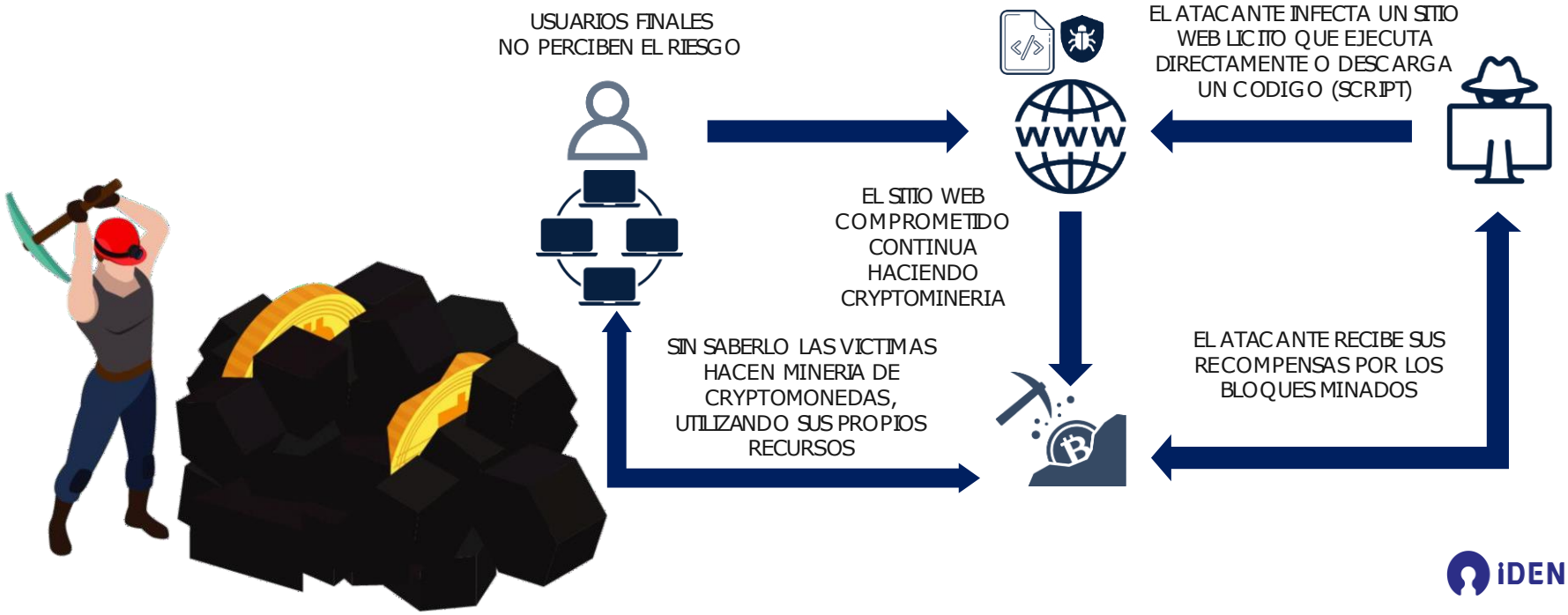


iDENTIAN®

PHISHING, FRAUDE, RIESGOS

CRYPTOJACKING

*El **cryptojacking** (también denominado minería de criptomonedas maliciosa) es una amenaza emergente de Internet que se oculta en un ordenador o en un dispositivo móvil, y utiliza los recursos de la máquina para "extraer" diversas formas de monedas digitales como criptomonedas*

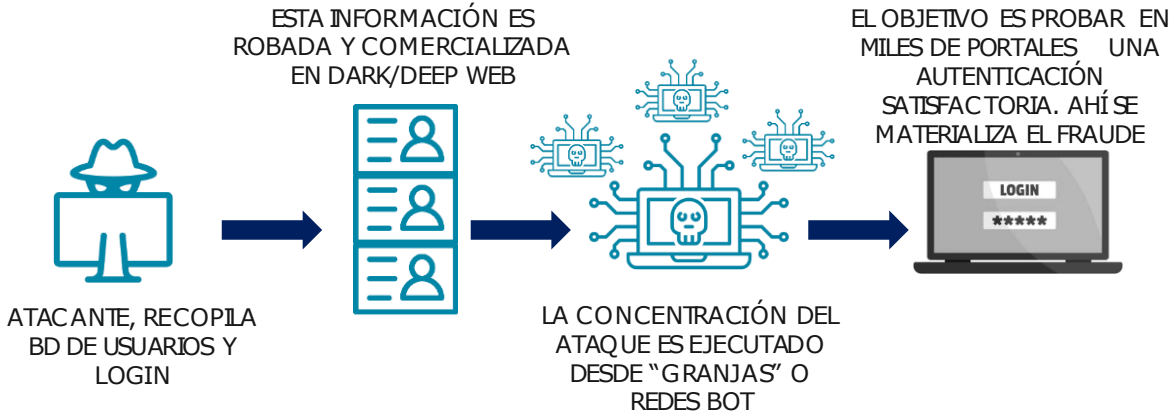


IDENTIAN®

PHISHING, FRAUDE, RIESGOS

CREDENTIAL STUFFING

*"**Credential stuffing**" es un tipo de ataque en el que de manera automatizada los atacantes prueban pares de nombres de usuario y contraseñas extraídas de alguna filtración con el fin de obtener acceso a una cuenta, también se aprovecha del reciclaje de credenciales que usualmente hacemos como usuarios*



IDENTIAN®

DUMPSTER DIVING (TRASHING)

También conocido como "***Trashing***" (***Buscar en la Basura***), es otro método de Ingeniería Social.
Mucha información puede ser encontrada en la basura.

IDENTIAN®

SUPLANTACION

Consiste en caracterizar a una persona o un rol. Generalmente los roles más empleados son **soporte técnico, gerente, encuestador, mensajero, etc.**

En empresas grandes es difícil conocer a todos los empleados y falsificar las ID resulta Muy Simple!

IDENTIAN®

CURIOSIDAD (Hardware)

El atacante deja un ***dispositivo de almacenamiento*** co mo pendrive, CD, memoria USB en un lugar donde pueda ser encontrado, mientras espera a que la víctima introduzca el dispositivo para infectarse con el código malicioso.

A través de la ***curiosidad*** humana es posible llevar a cabo este tipo de ataque.

IDENTIAN®

SHOULDER SURFING

Consiste en espiar por encima del hombro y realiz ar ***notas mentales*** sobre las teclas que presiona el usuario al momento de ingresar sus datos de acceso a un sistema.

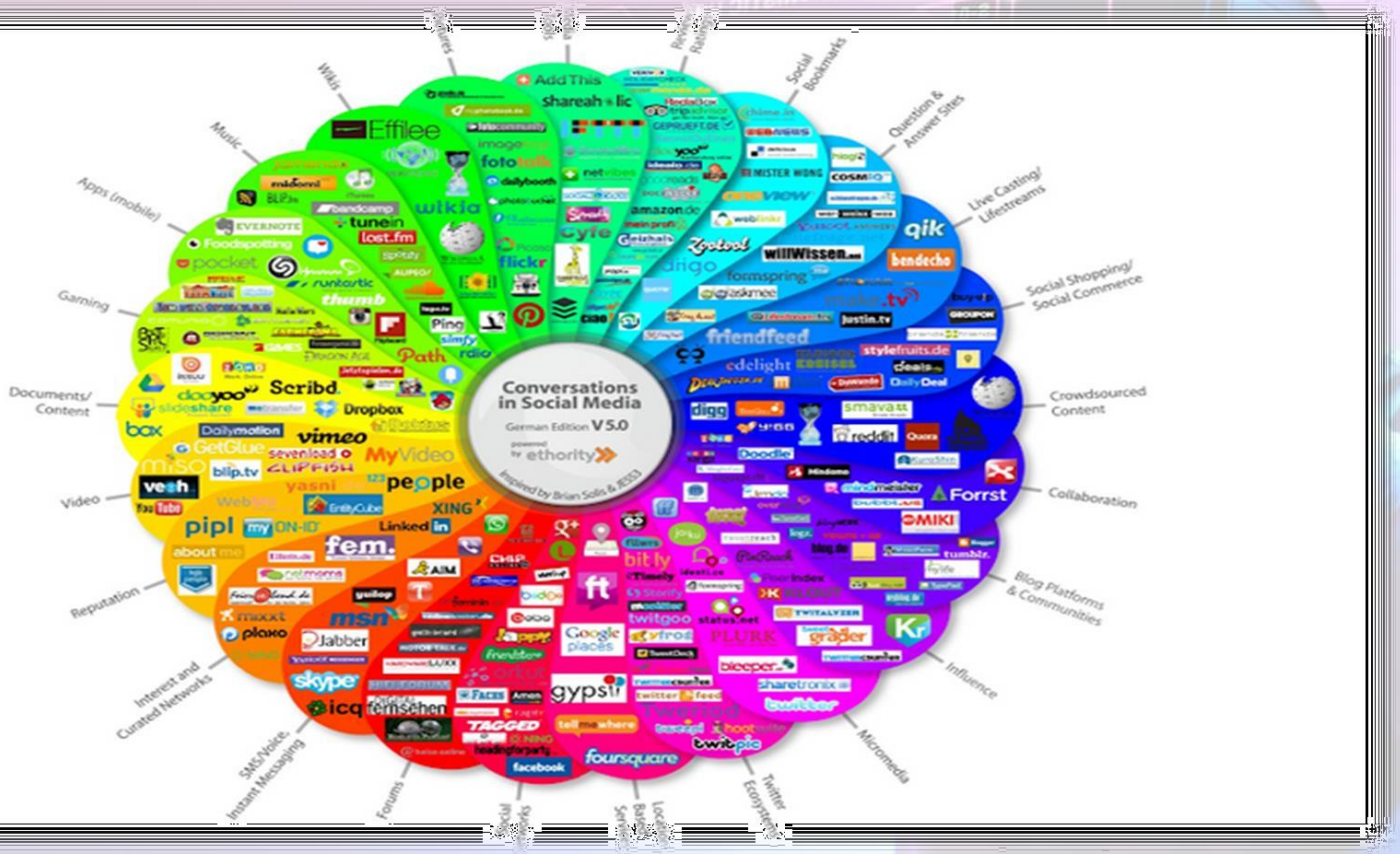
5. RIESGOS VS IA/MACHINE LEARNING/ BIGDATA

METAVERSO

* Realidad aumentada
* 3D
* Realidad virtual
* Crypto y NFT

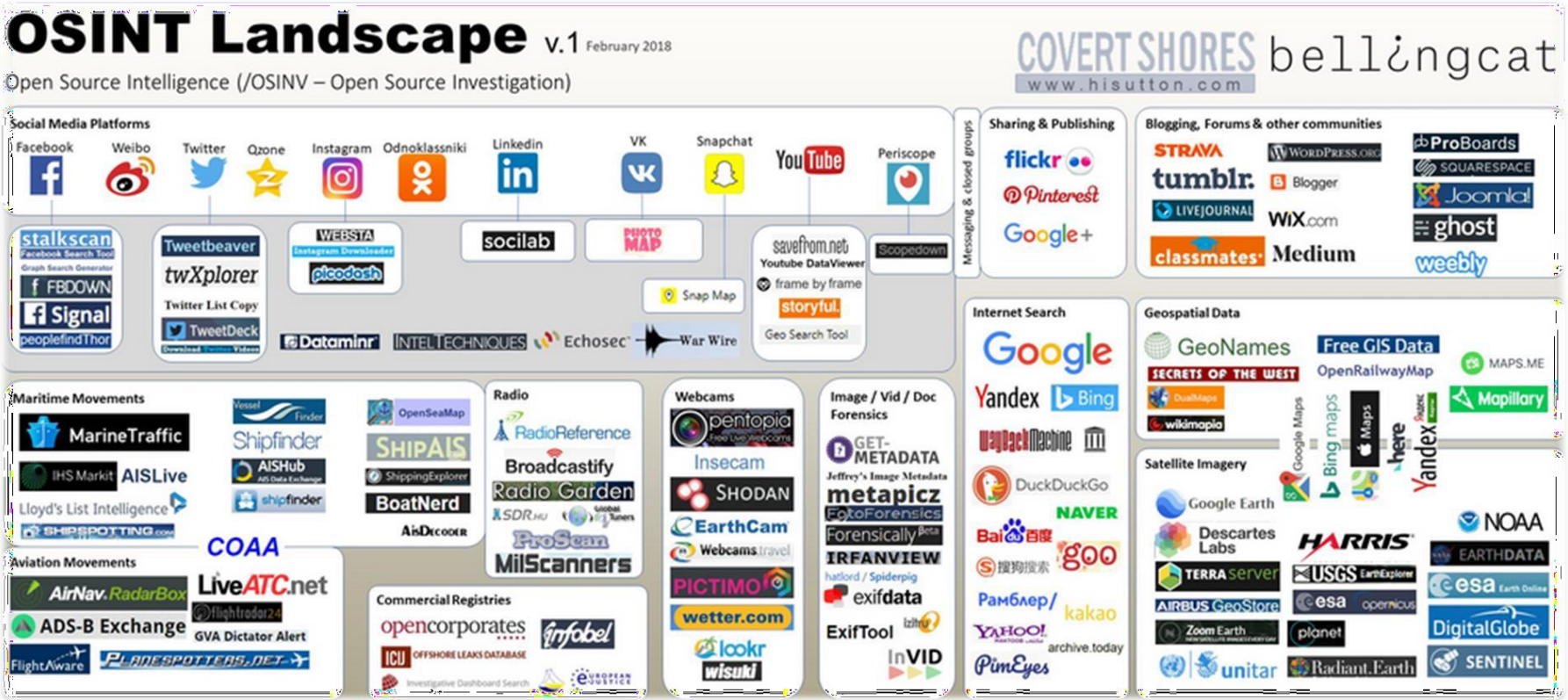
IDENTIAN®

RIESGOS VS IA/MACHINE LEARNING/ BIGDATA



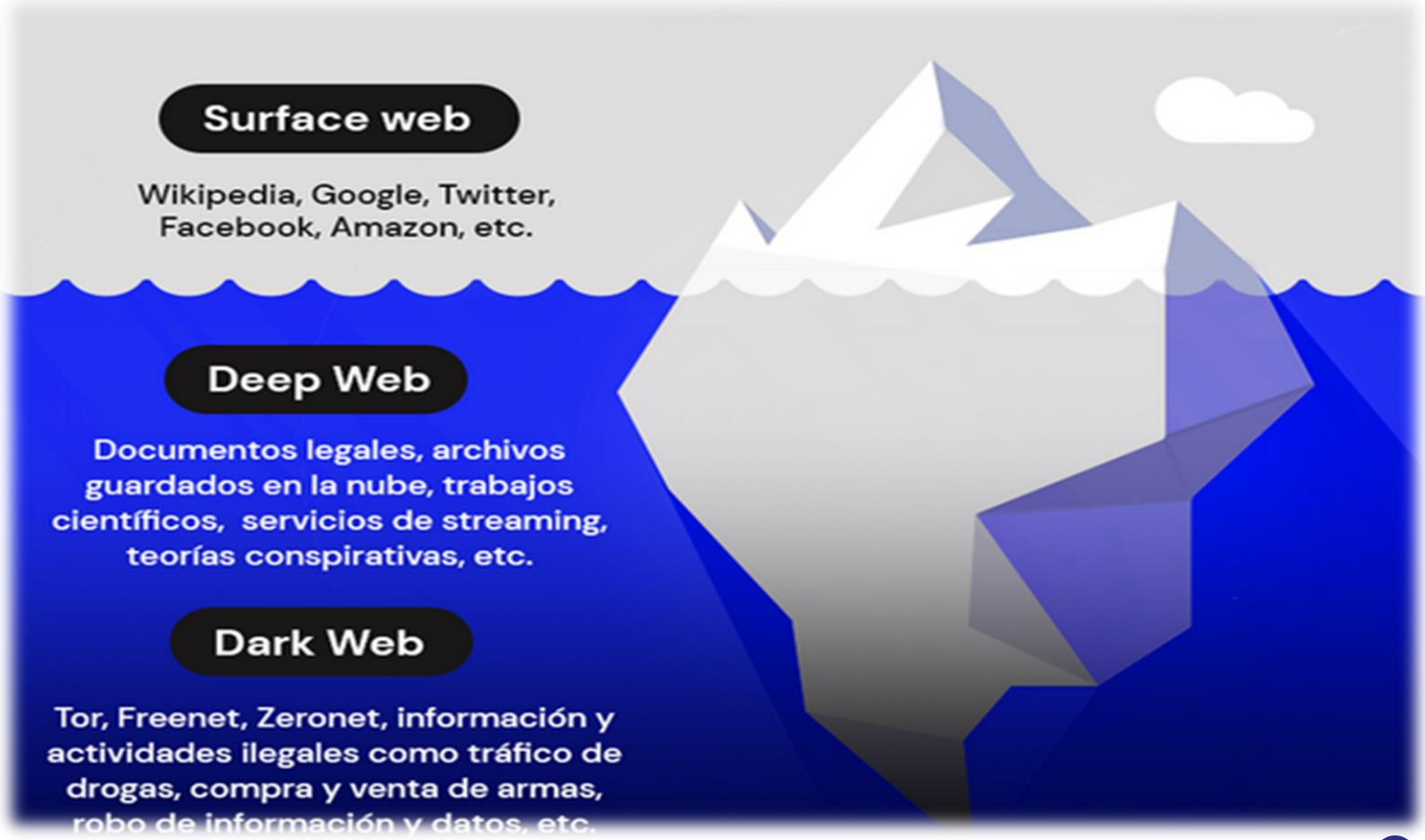
iDENTIAN®

RIESGOS VS IA/MACHINE LEARNING/ BIGDATA



iDENTIAN®

RIESGOS VS IA/MACHINE LEARNING/ BIGDATA



6. HACKERS DESMITIFICANDO EL MISTERIO

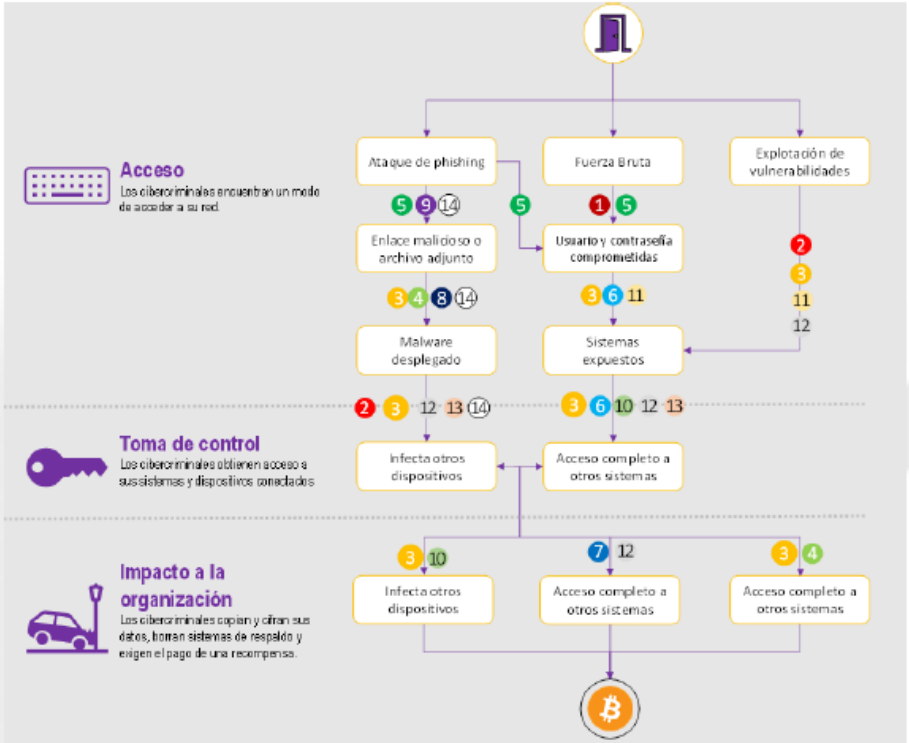
ANATONIA DE UN ATAQUE

ANATONIA DE UN ATAQUE

IDENTIAN®

ANATOMÍA DE UN ATAQUE

¿Cómo ocurre un incidente de ransomware y cómo prevenirlos?



1. Password Manager
2. Actualización y parches
3. Configuración de logs y alertas
4. Autorización de aplicaciones
5. Entrenamiento en ciberseguridad
6. Autenticación multifactor
7. Respaldos/Backups
8. Deshabilitar macros
9. Protección de dominio email
10. Principio de mínimo privilegio
11. Exposición segura a internet
12. Segmentación de redes
13. Herramientas de seguridad (AV,AM Firewall)
14. Protección del DNS

IDENTIAN®

ANTE EL MERCADO	ANTE LOS CLIENTES	GESTIÓN ORGANIZACIÓN
Afianza la posición de su organización	Mayor confianza del cliente	Seguridad
Nuevos clientes	Aumenta satisfacción	Servicios TI orientados hacia el negocio. Eficiencia y productividad
Factor competitivo	Mejor imagen y comunicación	Conocimiento y depuración procesos internos
Imagen de marca	Confidencialidad, Integridad y Disponibilidad de la información	Mejor gestión de recursos y costes
Favorece el desarrollo	Gestión de la continuidad de	Mejora continua
Puntúa en pliegos de las AAPP.		

7. ESTRATEGIAS DE CIBERSEGURIDAD

IDENTIAN®

MEDIDAS DE PREVENCIÓN Y PROTECCIÓN

1. Copias de seguridad

   Realizar copias de seguridad regulares y almacenarlas en un lugar seguro.

2. Software de seguridad

   Instalar y mantener actualizados programas antivirus y antimalware.

3. Educación y concientización

   Brindar capacitación a los empleados para reconocer y evitar ataques de ransomware.

4. Actualizaciones de software

   Mantener todos los programas y sistemas operativos actualizados con los últimos parches de seguridad.

ACCIONES A TOMAR SI SE ES VÍCTIMA DE RANSOMWARE

Reportar el incidente

Contactar a las autoridades y proporcionar toda la información relevante sobre el ataque.

No pagar el rescate

Pagar el rescate no garantiza la recuperación de los datos y puede fomentar futuros ataques.

Consultar a expertos

Buscar ayuda de profesionales en ciberseguridad para evaluar las opciones de recuperación de datos.

IDENTIAN®

CONCLUSIONES Y RECOMENDACIONES

Importancia de la seguridad

El ransomware destaca la necesidad de tener medidas de seguridad robustas para proteger nuestros datos.

Prevención y educación

La prevención y la educación son clave para protegerse contra los ataques de ransomware.

Colaboración y concientización

Es responsabilidad de todos trabajar juntos para crear un entorno cibernético seguro.

IDENTIAN®

REGULACIONES DEL SECTOR COLOMBIA CIBERSEGURIDAD

ISO 27001

Ley 1581 de 2012
Reglas generales para el tratamiento de datos personales

ISO 28001 – Seguridad de la cadena de suministro

Documento
CONPES
3995

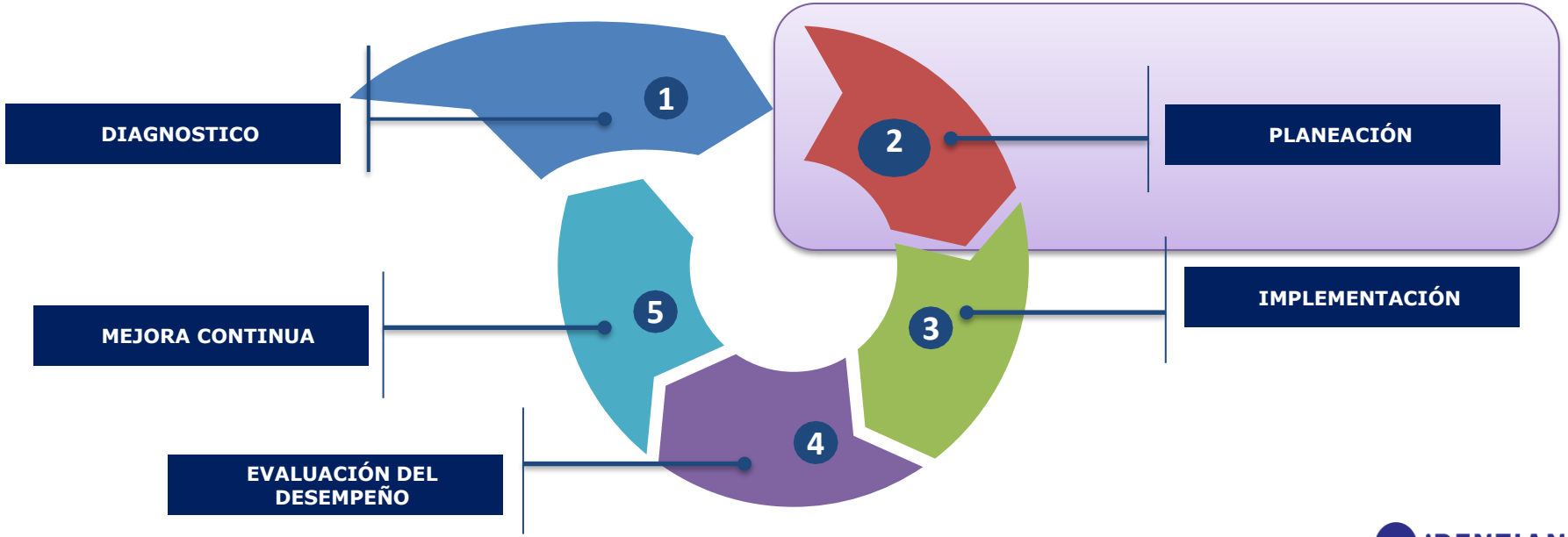
CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL
REPÚBLICA DE COLOMBIA
DEPARTAMENTO NACIONAL DE PLANEACIÓN

HIPAA
Health Insurance Portability & Accountability Act

POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL

IDENTIAN®

ESTRATEGIAS DE CIBERSEGURIDAD



Fuente: Modelo de Seguridad y Privacidad, MINTIC, Pág. 1-2

El modelo de seguridad de la información se estructura según la definición estratégica del Sistema de Gestión de Seguridad de la Información ISO 27001:2013

1	2	3	4	5
DIAGNOSTICO	**PLANEACIÓN**	**IMPLEMENTACIÓN**	**EVALUACIÓN DEL DESEMPEÑO**	**MEJORA CONTNUA**
				
Identificar el estado actual con respecto a la seguridad de la información y ciberseguridad.	**En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.**	**ORGANIZACIONES planifica, implementa y controla los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.**	**Requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información**	**Proceso de mejora del modelo de seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan**

IDENTIAN®

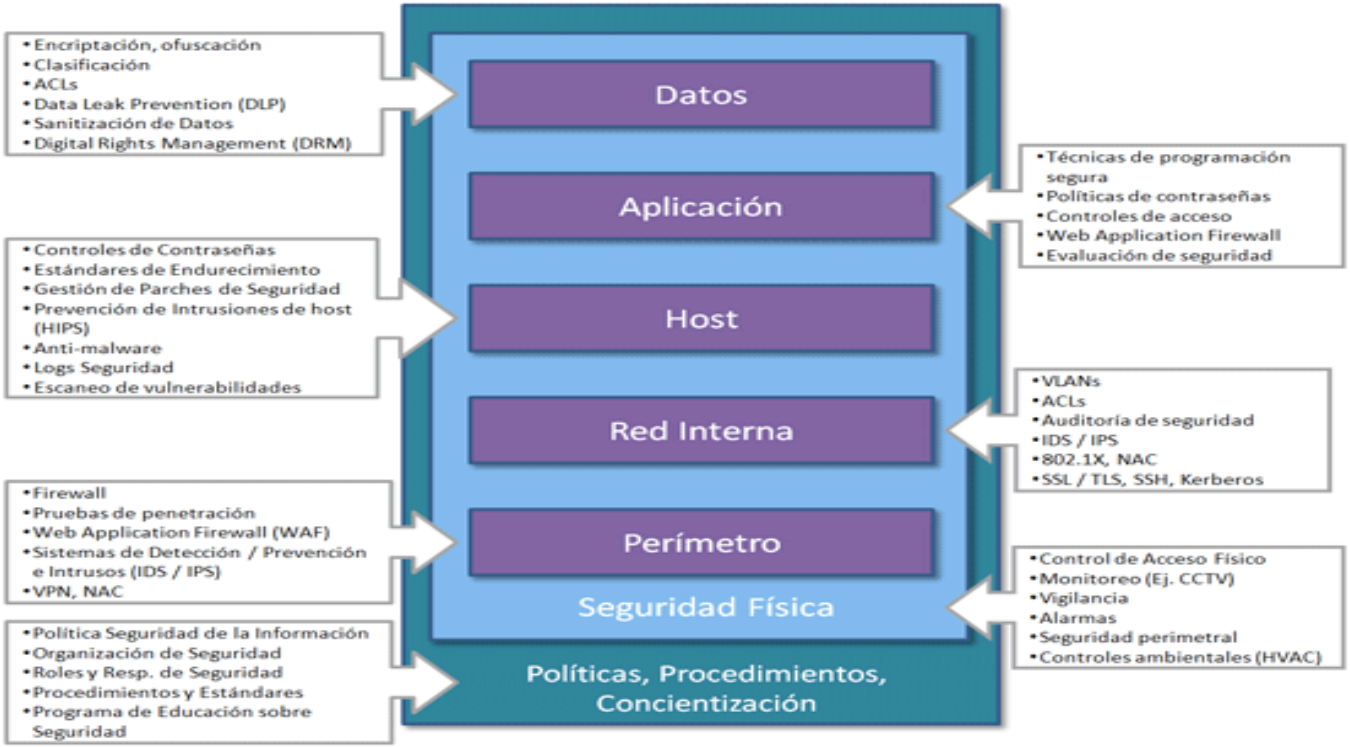
PLAN DE RUTA CIBERSEGURIDAD

IDENTIAN®

INICIATIVAS Y PROYECTOS

IDENTIAN®

INICIATIVAS Y PROYECTOS



IDENTIAN®

GRACIAS!!!

dirección@identian.co
info@identian.co

IDENTIAN®