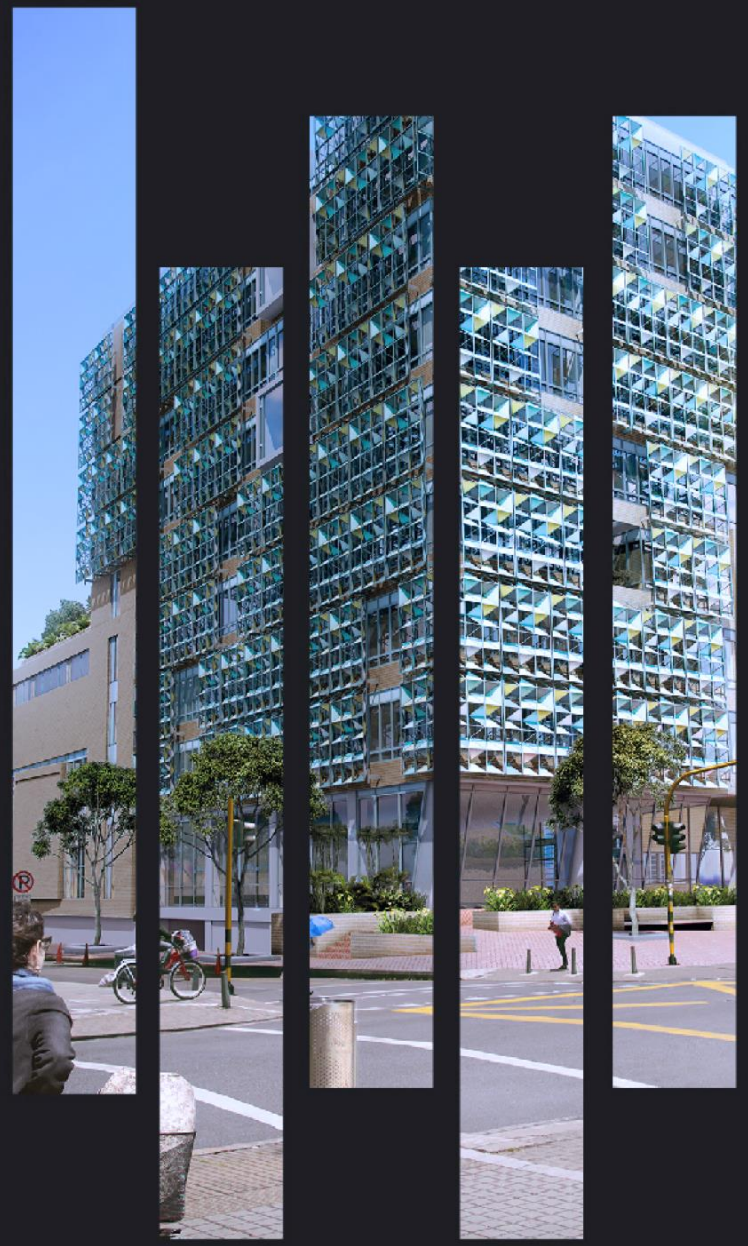


ean universidad

Acreditada en Alta Calidad
Res. nº. 29499 del Mineducación. 29/12/17 vigencia 28/12/21

Ciberseguridad y Compliance

Juanita Rodríguez Kattah
Vicerrectora de Innovación

Estrategias Nacionales: Seguridad y Confianza Digital

- 1. Institucionalidad
- 2. Educación en Seguridad de la Información
- 3. Fortalecimiento de la legislación en materia de ciberseguridad

- 1. Múltiples partes interesadas
- 2. Responsabilidad compartida
- 3. Enfoque en Gestión de Riesgos Cibernéticos

Institucionalidad en materia de **Seguridad Digital**

Coordinador nacional: Presidencia de la República

Investigación y respuesta ante delitos cibernéticos	Salvaguardar los intereses nacionales en el ciberespacio	Coordinar a nivel nacional en aspectos de ciberseguridad y ciberdefensa	Conciencia ciudadana líder de la política e seguridad digital para Gobierno	Judicialización	Primer CSIRT sectorial, CSIRT de Gobierno	Inteligencia estratégica del Estado

CSIRTs Sectoriales: Financiero – Eléctrico

Centro de Capacidades y Ciberseguridad de Colombia – C4

Comité de Seguridad Digital

Responsabilidad compartida

Gobierno

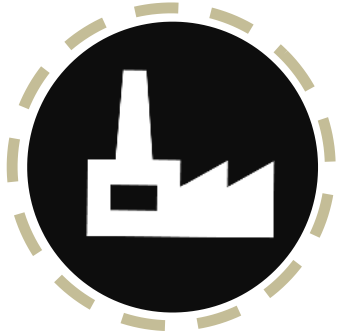
1 Promover capacidades para la Gestión de riesgos

Ciudadano

2 Acatar recomendaciones

3 Adelantar acciones preventivas y correctivas (actualizaciones de software, parcheos)

Sector Privado



4 Reportar incidentes

¿Por qué hablar de **Ciberseguridad y Compliance**?

Generar Confianza

- **Adaptación al medio**: Sistemas de información con base tecnológica están presentes en todos los procesos de cualquier empresa
- Oportunidad de **crecimiento** y **mayores riesgos**
- Gestionar niveles adecuados de seguridad, a nivel de compliance y de alcance estratégico en la organización.

¿Cómo enfocar la Ciberseguridad en el ámbito del Compliance?

- El valor no solo está en la tecnología y la información.
- Integridad de las personas y su vínculo con el cumplimiento normativo: **Seguridad interna y seguridad con externos**.
- Protección de activos estratégicos y continuidad del negocio.
- Aprovechamiento de la información obtenida por **Fuentes abiertas**

Ciberseguridad,
Conclusión:

1. Herramienta para la seguridad empresarial y/o corporativa, o protección frente a amenazas:
   - Estructurales.
   - Económicas.
   - Información (disponibilidad, integridad y confidencialidad).
2. Herramientas para el cumplimiento de legislación, normativa, buenas prácticas, etc.:
   - Responsabilidad penal.
   - Responsabilidad civil.
   - Responsabilidad administrativa
3. Factor diferencial y generador de confianza.

Seguridad legal, normativa y buenas prácticas

1. Leyes y Normas:

    - Protección de datos personales.
    - Leyes y normativas relacionadas con la sociedad de la información, comercio electrónico, etc.
    - Propiedad intelectual.
    - Transparencia y buenas prácticas
    - Otras normas específicas del sector, así como generales de aplicación.
    - Etc.

2. Seguridad con terceros.

3. Seguridad interna con empleados.

¿Cómo lograrlo?

Análisis de Seguridad

1. Punto de Partida
2. Procesos críticos, empleados, equipos, activos..
3. **Legislación aplicable**

Nivel u objetivo de seguridad

1. Nivel de seguridad
2. Sector, tipo de negocio, requisitos del negocio/mercado, objetivos estratégicos.

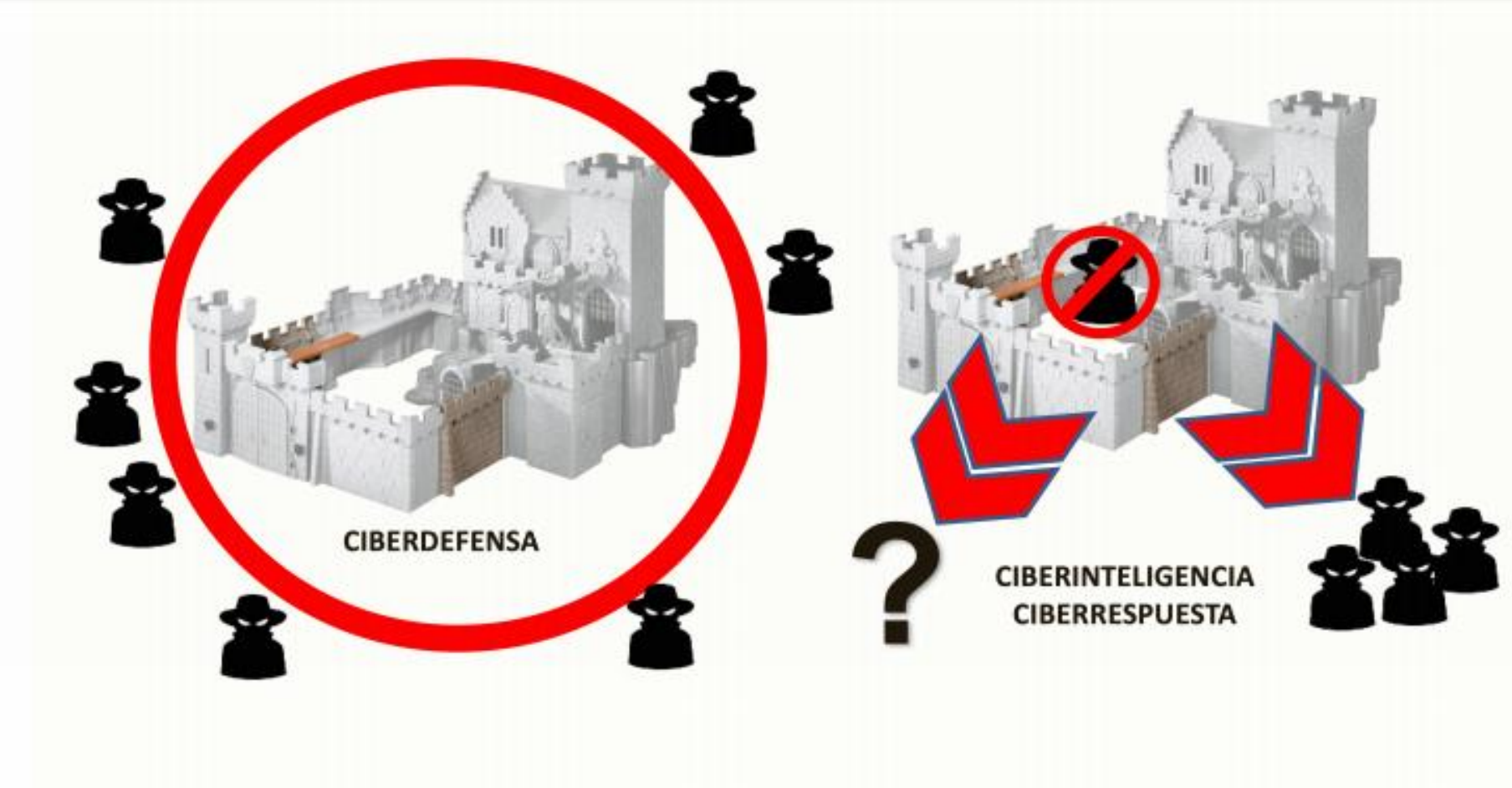
Riesgos

Plan Director de Ciberseguridad

Normativas y procedimientos

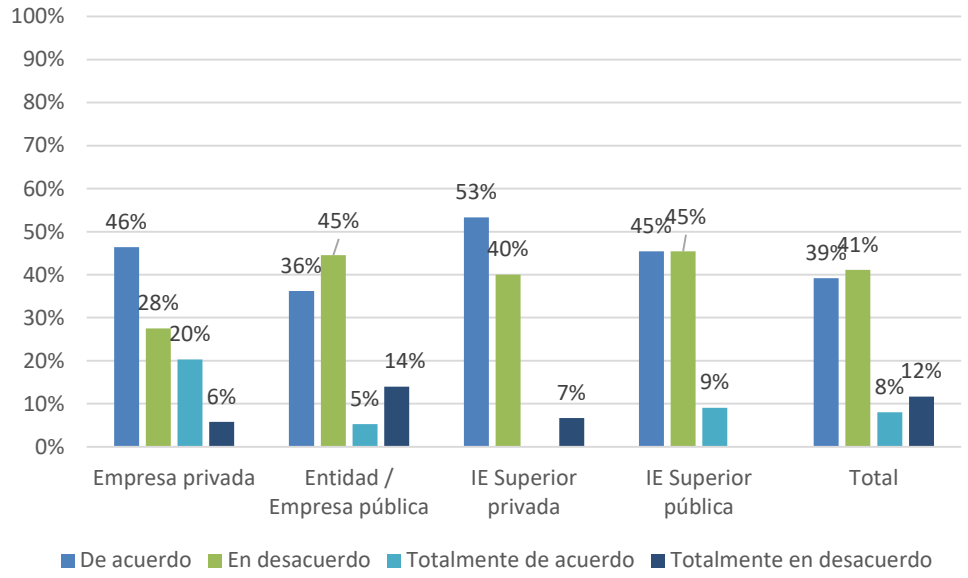
ean universidad

Comprendiendo los términos

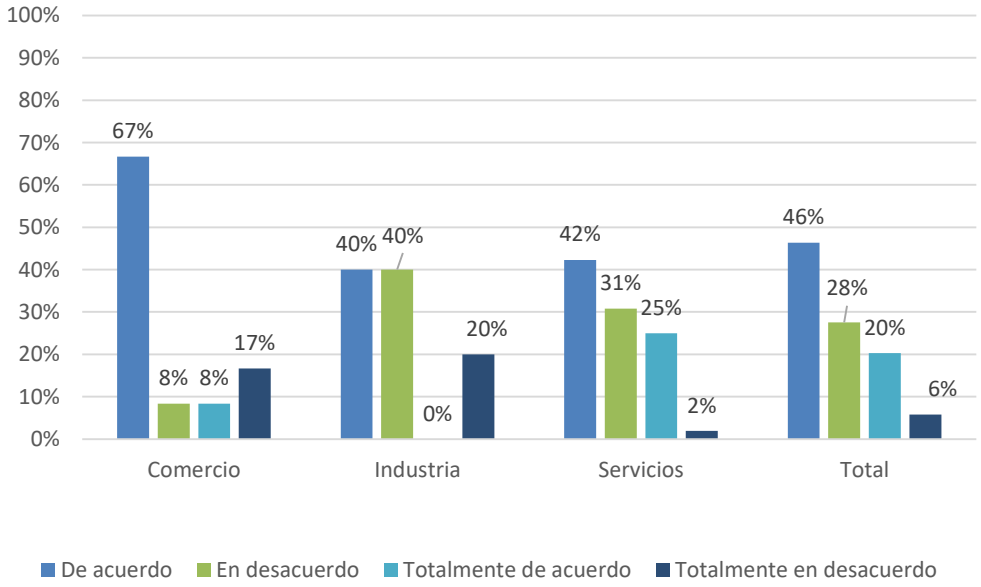


¿Mi organización está preparada para hacer frente a un incidente digital?

Por tipo de organización



Por tipo de EMPRESA PRIVADA

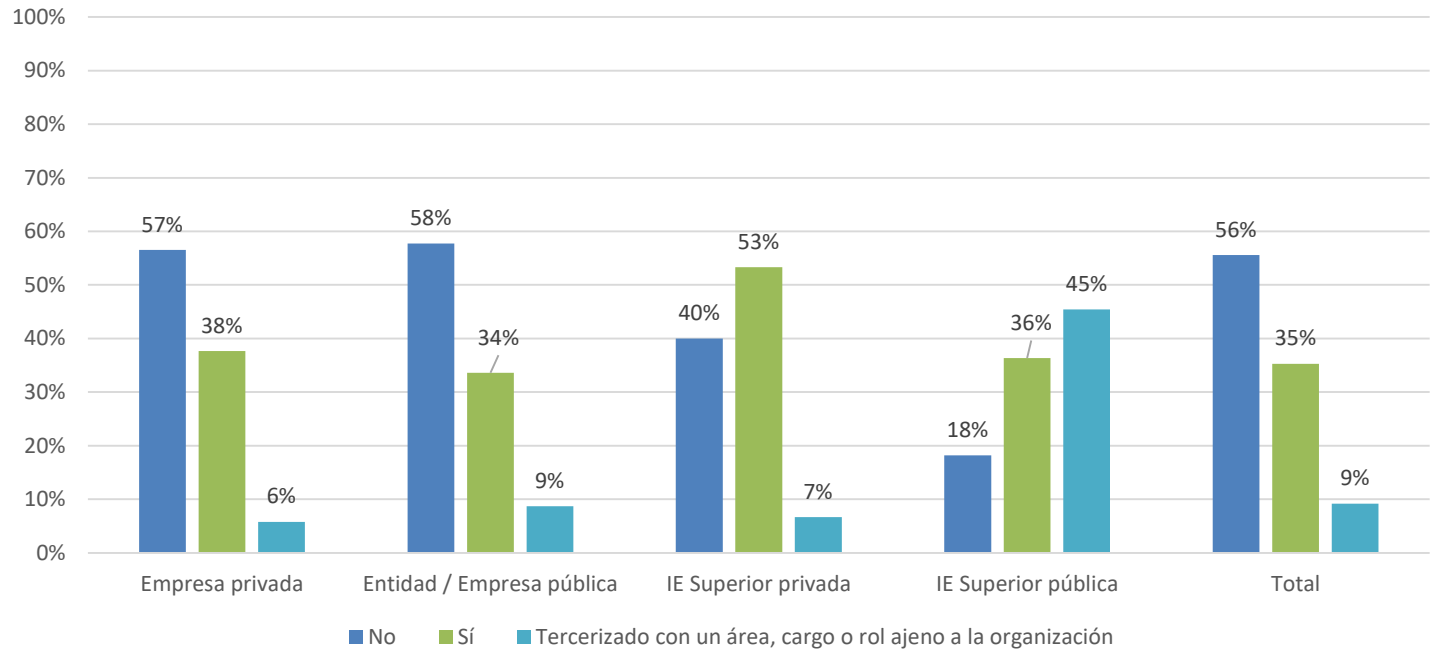


En 2017 tan sólo el 16,6% de las empresas contaba con protocolos para dar respuesta a incidentes de seguridad digital

Fuente: SG/OEA a partir de información recolectada de organizaciones y universidades en Colombia

¿Tiene un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital?

Por tipo de organización

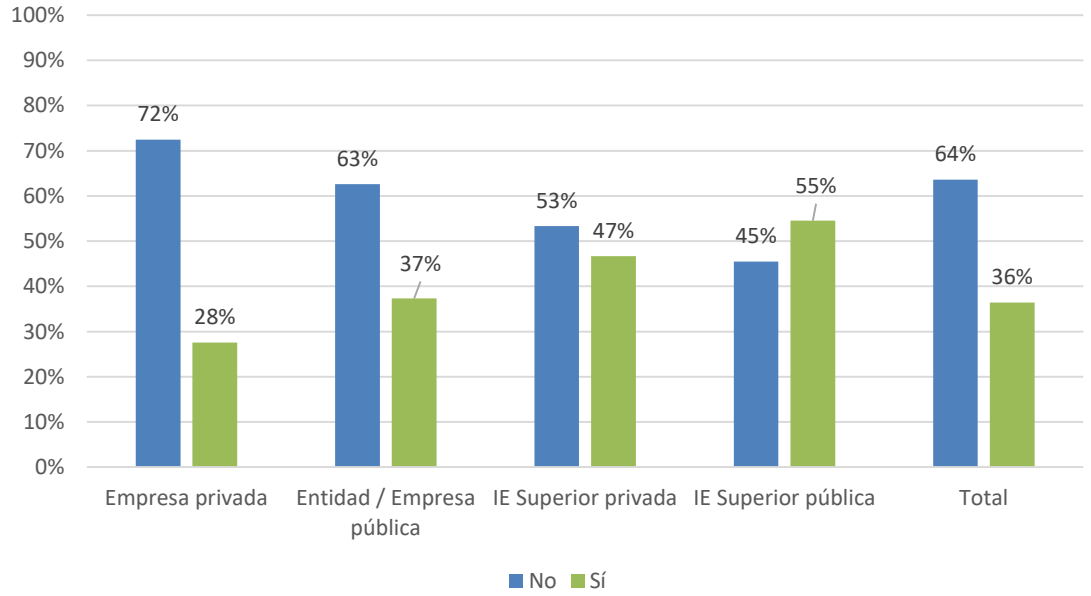


En 2017 tan sólo el 17,5% de las empresas colombianas tenia un cargo o rol dedicado a la seguridad digital

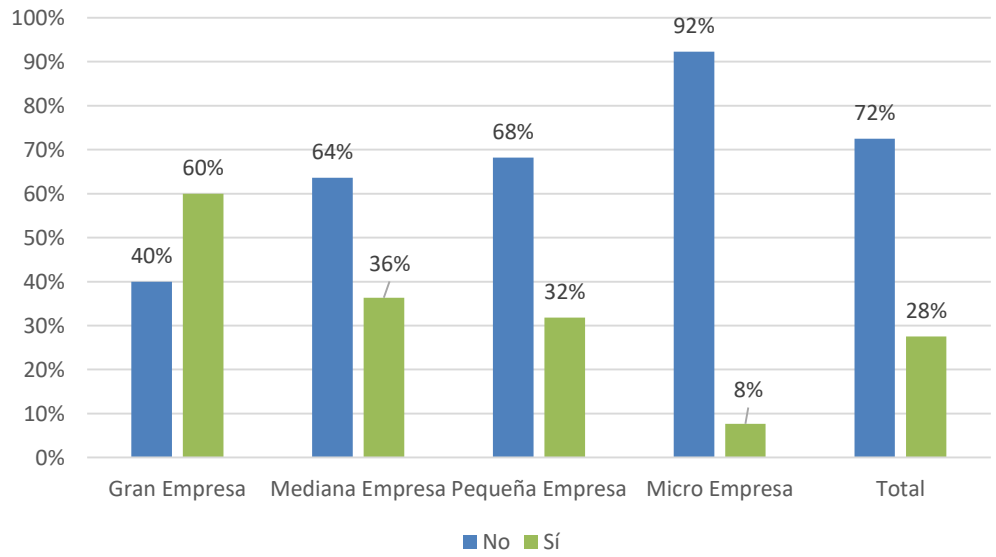
Fuente: SG/OEA a partir de información recolectada de organizaciones y universidades en Colombia

¿Su organización ha identificado amenazas de seguridad digital en los últimos 12 meses?

Por tipo de organización



Por tamaño de EMPRESA PRIVADA



En 2017 tan sólo el 5,2% de las empresas reveló que tuvo incidentes de seguridad digital (Grandes: 17,7%, Mediana: 11,4%, Pequeña: 9,4% y Micro: 2,9%)

Fuente: SG/OEA a partir de información recolectada de organizaciones y universidades en Colombia

RETO:
Seguridad y Resiliencia

GRACIAS

Juanita Rodríguez Kattah
jrodriguezk@universidadean.edu.co
@jrodriguezk

ean universidad

Acreditada en Alta Calidad
Res. nº. 29499 del Mineducación. 29/12/17 vigencia 28/12/21

www.universidadean.edu.co

Centro de contacto en Bogotá: (57-1) 5936161 - (57-1) 5400330 - (57-1) 6398910
Línea gratuita nacional 01 8000 93 1000
E-mail: informacion@universidadean.edu.co
Cl. 79 Nº. 11 - 45 El Nogal, Bogotá D.C. Colombia, Suramérica

CIBERDELITO EN EPOCAS DE PANDEMIA

JOHN JAIRO ECHEVERRY ARISTIZABAL
Ingeniero de Sistemas
Especialista en Telecomunicaciones
Master en Auditoría, Seguridad Gobierno y Derecho de las TICs

DISEÑADO PARA …

ESTA CHARLA ESTA DISEÑADA PARA LOS OFICIALES DE CUMPLIMIENTO DE EMPRESAS DEL SECTOR REAL, EN DONDE SE EXPLICARÁN LAS TIPOLOGÍAS DE CIBERDELITO QUE SE VIENEN DANDO EN NUESTRO PAÍS, ESTO, FRENTE A LA UTILIZACIÓN DE TI (TECNOLOGÍAS DE LA INFORMACIÓN), ESPECIALMENTE, EN EL CONTEXTO QUE ESTAMOS VIVIENDO EN LA ACTUALIDAD -COVID 19-, Y CON ELLO, GENERAR ESTRATEGIAS CORPORATIVAS FRENTE A CIBERSEGURIDAD.

EL CIBERDELITO ....

CIBERSEGURIDAD

GESTIÓN DE RIESGOS

CIBERDELITO

El CIBERDELITO ...

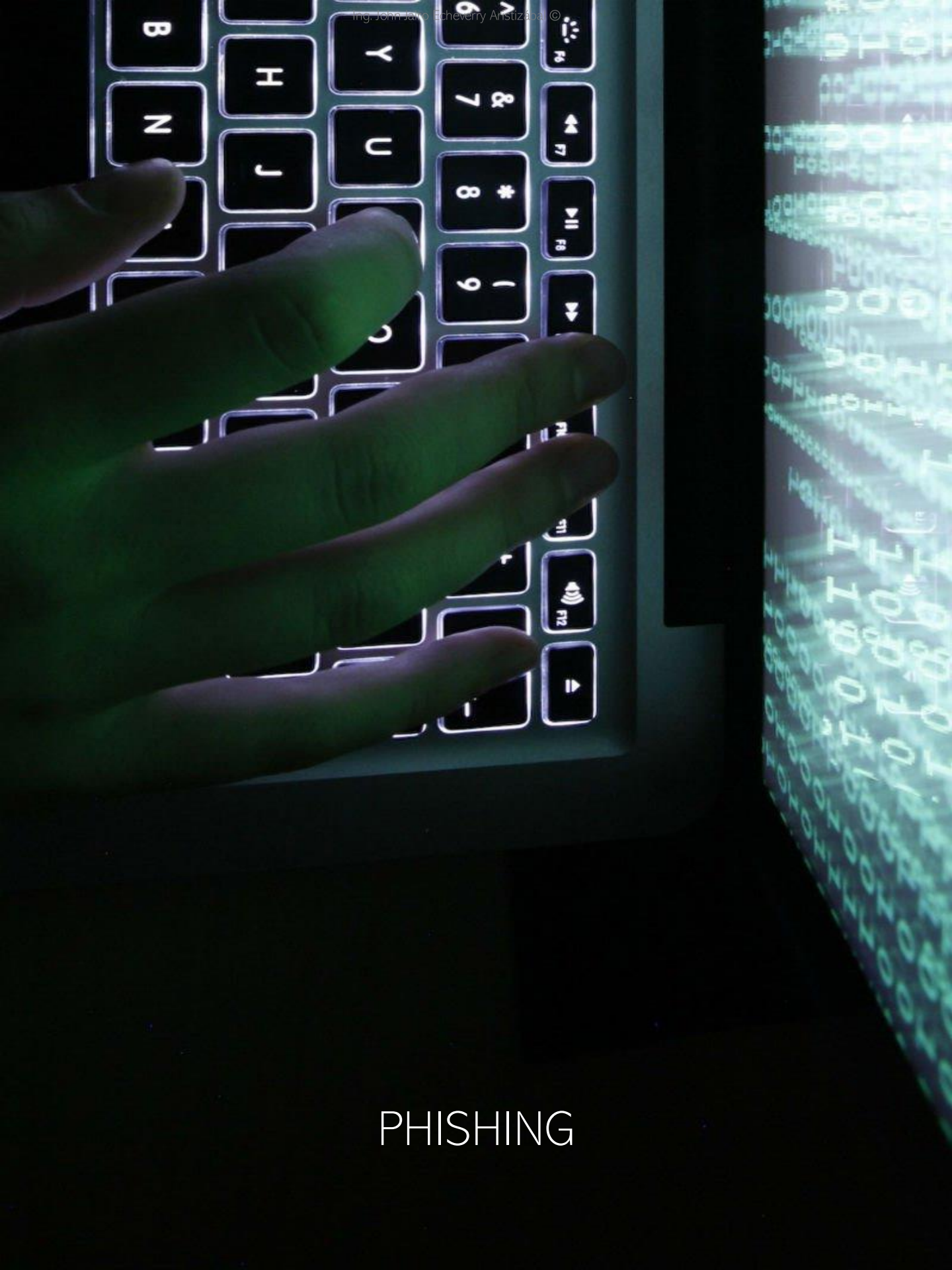
Los avances Tecnológicos demuestra la evolución del hombre, esto se evidencia a través de los medios que permiten el almacenamiento, la transmisión y la administración de la información; avances que han modificado el vivir diario de las personas y organizaciones reflejado esto, en el aumento de transacciones comerciales (cajeros automáticos, banca virtual), comercio electrónico, comunicaciones en línea, sistemas de información, etc., actividades que han permitido mejorar ostensiblemente procesos al interior de las organizaciones; pero así mismo, se han generado una serie de comportamientos ilícitos aprovechando el conocimiento de ésta tecnología lo cual se denomina "**DELITOS INFORMÁTICOS**" y su evolución "**CIBERCRIMEN**"

Ing. John Jairo Echeverry Aristizábal ©

SU DEFINICIÓN …

SON TODAS LAS CONDUCTAS ILÍCITAS REALIZADAS POR UN SER HUMANO, SUSCEPTIBLES DE SER SANCIONADAS POR EL DERECHO PENAL EN DONDE HACEN UN USO INDEBIDO DE CUALQUIER MEDIO INFORMÁTICO PARA OBTENER LA INFORMACIÓN O LOS DATOS DE CARÁCTER PRIVADO DE UN INDIVIDUO, CON EL PROPÓSITO DE LOGRAR UN BENEFICIO.

VENTAJAS DE LA TECNOLOGÍA



PHISHING

PHISHING

T

E

Es la suplantación de sitios *web* conocidos, para capturar datos privados y semi privados de personas y/o organizaciones.

M

El ciberdelincuente envía enlaces (*links*) a través de medios digitales (redes sociales y/o correos electrónicos) que son bastantes llamativos para el cibernauta.

E

Ochocientos (840) casos registrados en el primer semestre del 2020, que frente al mismo periodo del año 2019, aumento un 240% *

* Estadística tomada del informe de tendencias de Cibercrimen Primer trimestre 2020 Policía Nacional TICTAC y SAFE

Phishing de Clonado o Direccionamiento

El Ciberdelincuente se hace pasar por alguien conocido o por una marca que cuenta con la confianza de la victima

Smishing

Es un tipo de phishing que no se realiza mediante suplantación de sitios web, ni correos electrónicos, sino utilizando teléfonos móviles. Se hace pasar por una empresa de confianza y envía SMS con información de interés.

Vishing

El hacker establece centros de atención telefónica directamente lanza llamadas haciéndose pasar por algún proveedor u operadora de dentro de soporte

Búsquedas de navegador

Consisten en posicionar una pagina falsa por encima de la oficial, esto mediante técnicas SEO.

Spear Phishing

Es un ataque mas personalizado, en donde a través de redes se hace una perfilación de la victima (correo electrónico, Smartphone)

Suplantación CEO

Consiste en hacerse a las credenciales del CEO o de cualquier otra persona con un cargo relevante de la empresa, y así, enviar correos electrónicos solicitando datos confidenciales o acciones financieras.

Malware basado en Phishing

Es un ataque que e caracteriza por el envío de correos electrónicos en los que se introduce una pieza de malware como archivo adjunto descargable

CAPTURA DE DATOS PERSONALES

CAPTURA DE DATOS PERSONALES

T

E

Es el apoderamiento de información semiprivada, privada o sensible de personas y/o organizaciones a través de medios digitales.

M

Mediante técnicas de engaño (ingeniería social) a través de redes sociales, correos electrónicos, o con la instalación de herramientas de *malware*, también conocido como *spyware* (software espía), el ciberdelincuente se apodera de datos personales y/o corporativos, y con ello, los emplea para su aprovechamiento, iniciando acciones extorsivas bajo la modalidad coercitivas.

E

Novecientos cincuenta y ocho (958) casos registrados en el primer semestre del 2020, que frente al mismo periodo del año 2019, a tenido un aumento del 13,5%*

* Estadística tomada del informe de tendencias de Cibercrimen Primer trimestre 2020 Policía Nacional TICTAC y SAFE

TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

T

E

Esta asociado a la obtención de información financiera (usuarios y contraseña) del cuenta habiente, y mediante canales electrónicos transfiere el dinero de la persona y/o organización a otra cuenta (*Money mules*).

M

Mediante la instalación de herramientas maliciosas (spyware) se captura la información financiera de persona u organización.

E

Cuatrocientos setenta y cinco (475) casos registrados en el primer semestre del 2020, con un aumento del 8,2% frente al 2019, evaluado en esta misma fracción de tiempo *

* Estadística tomada del informe de tendencias de Cibercrimen Primer trimestre 2020 Policía Nacional TICTAC y SAFE

ACCESO ABUSIVO A SISTEMAS INFORMÁTICOS

ACCESOS ABUSIVOS A SISTEMAS INFORMÁTICOS

T

E

Se trata de ingresos no autorizados a plataformas tecnológicas por parte de los ciberdelincuentes, aprovechando los débiles esquemas de seguridad de *TI* que existen en las organizaciones.

M

Mediante el escalamiento de privilegios sobre recursos de TI, y/o la instalación de herramientas maliciosas (spyware) se captura la información de la organización, la cual es utilizada para realizar otras modalidades delictivas.

E

Novecientas dieciséis (916) casos registrados en el primer semestre del 2020, sin embargo, frente al mismo periodo del año anterior, se observó una disminución del 1,3% *

* Estadística tomada del informe de tendencias de Cibercrimen Primer trimestre 2020 Policía Nacional TICTAC y SAFE

MALWARE

Virus o Worms

Son archivos que se instalan por el usuario y permanecen allí hasta su ejecución, y su único propósito es afectar y/o destruir la información del equipo basado en un tema de propagación.

Troyanos

Son archivos que tienen la apariencia de documentos normales pero esconden en su interior herramientas de malware que buscan la obtención de información y/o el apoderamiento del equipo.

Keyloggers

Son herramientas capaces de registrar todas las pulsaciones de teclado, y con ello, conseguir contraseñas.

Spyware

El objetivo de este malware, es el robo de información.

Adware

Esta modalidad se encarga de mostrar publicidad al usuario a través de banners, pop-ups, en donde en muchos casos el objetivo es obtener información sobre las actividades del usuario en la red

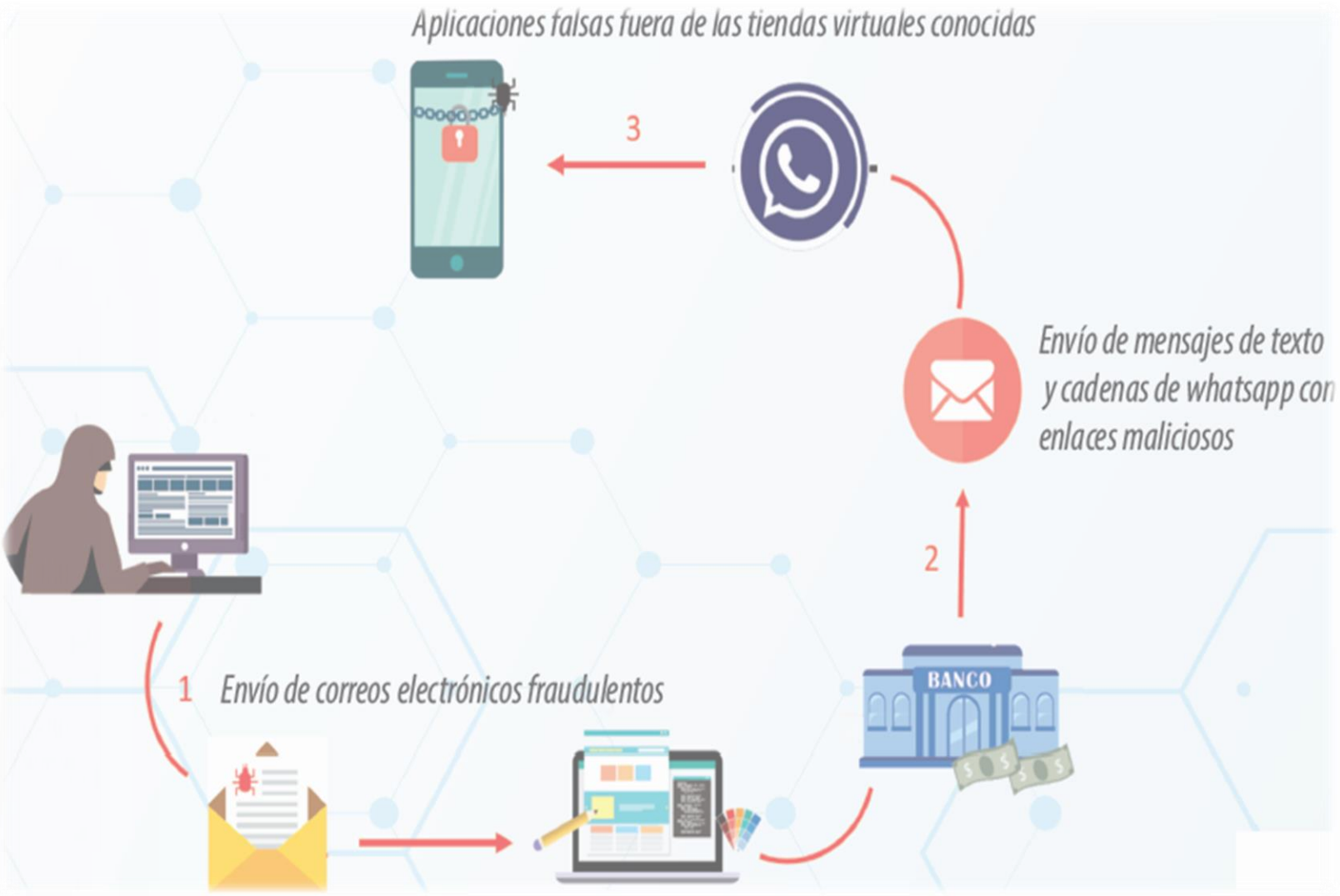
Ramsomware

Este tipo de ataque es uno de los más abunda en la actualidad, y se basa en el cifrado de datos, restringiendo el acceso a los archivos, generándose una extorsión digital, en donde se pide un rescate por la información.

Malware basado en Phishing

Es un ataque que se caracteriza por el envío de correos electrónicos en los que se introduce una pieza de malware como archivo adjunto descargable

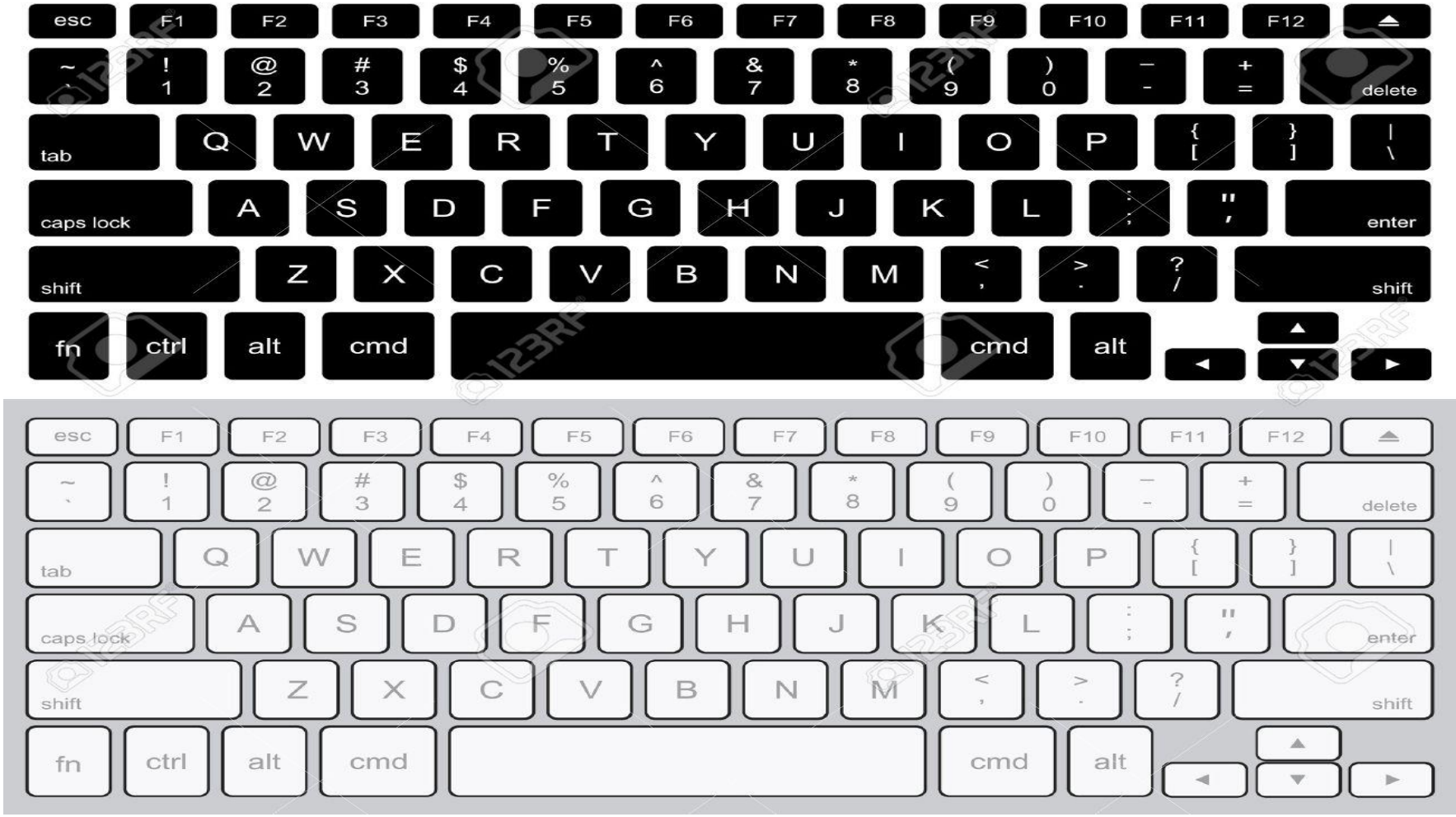
CARACTERIZACIÓN DEL FRAUDE



CARACTERIZACIÓN DEL FRAUDE….

CARACTERIZACIÓN DEL FRAUDE….

UN EJEMPLO ....



CONTROLES

Identificar cuales son los activos de información más importantes de la organización

¿Conozco los activos de información de mi organización?
¿Los he clasificado de acuerdo a su criticidad?
¿Tenemos una matriz de responsabilidad?

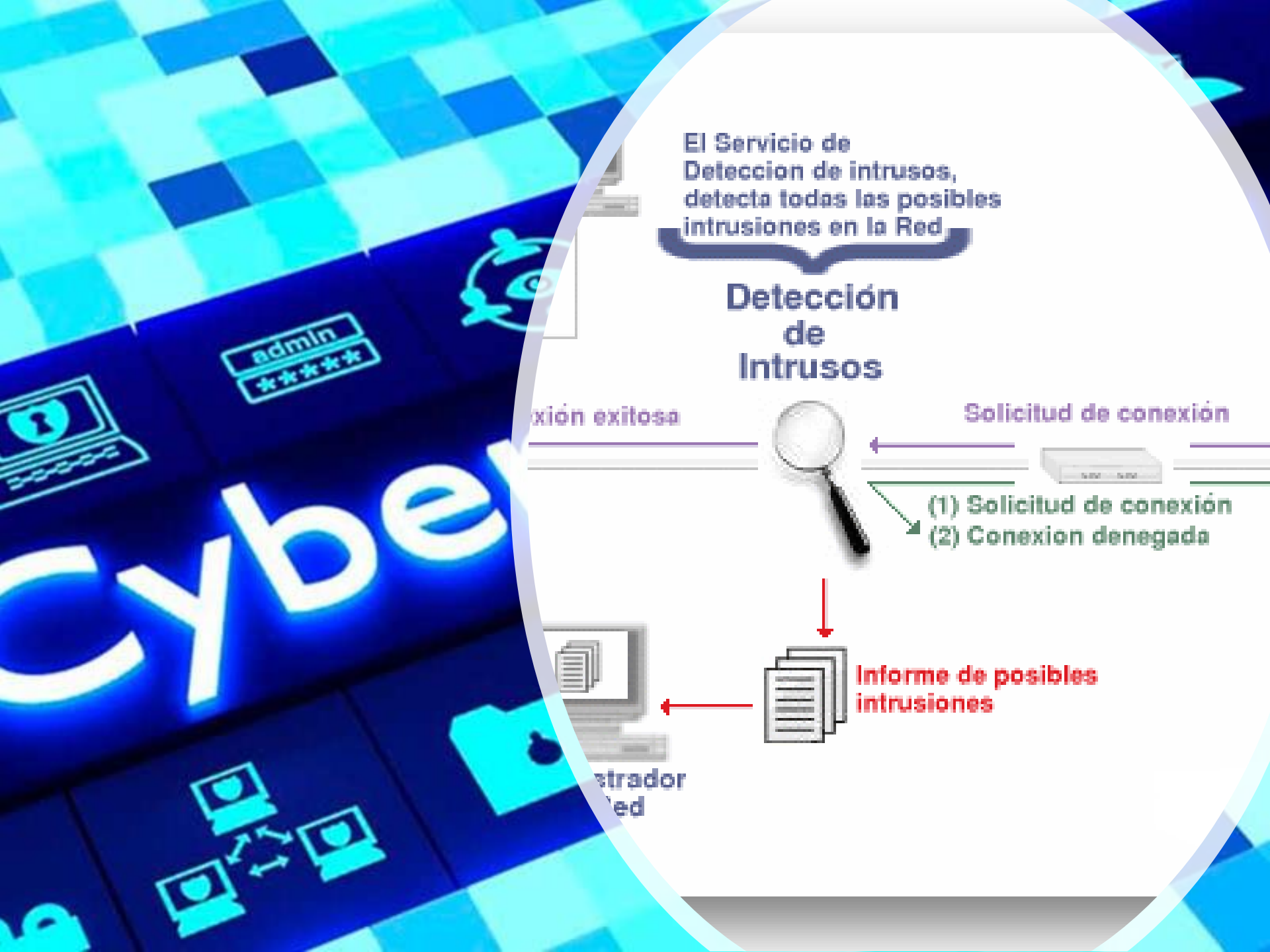
Realizar una Gestión de riesgos frente Ciberseguridad, seguridad informática y seguridad de la información

¿Conozco cuales son mis amenazas?
¿Distingo mis Vulnerabilidades?
Se han ponderado los riesgos de acuerdo a mi exposición?

Definir políticas complementarias frente Ciberseguridad, seguridad informática o seguridad de la información

¿Existen políticas de ciberseguridad?

- política para dispositivos móviles;
- política de teletrabajo;
- política de control de acceso;
- política de controles criptográficos;
- política de respaldo de información;
- política de transferencia de información;
- política de desarrollo seguro de software;
- política de relación con proveedores;
- política de protección de datos personales.


admin
*****
El Servicio de
Deteccion de intrusos,
detecta todas las posibles
intrusiones en la Red
Detección
de
Intrusos
Solicitud de conexión
(1) Solicitud de conexión
(2) Conexion denegada
Informe de posibles
intrusiones

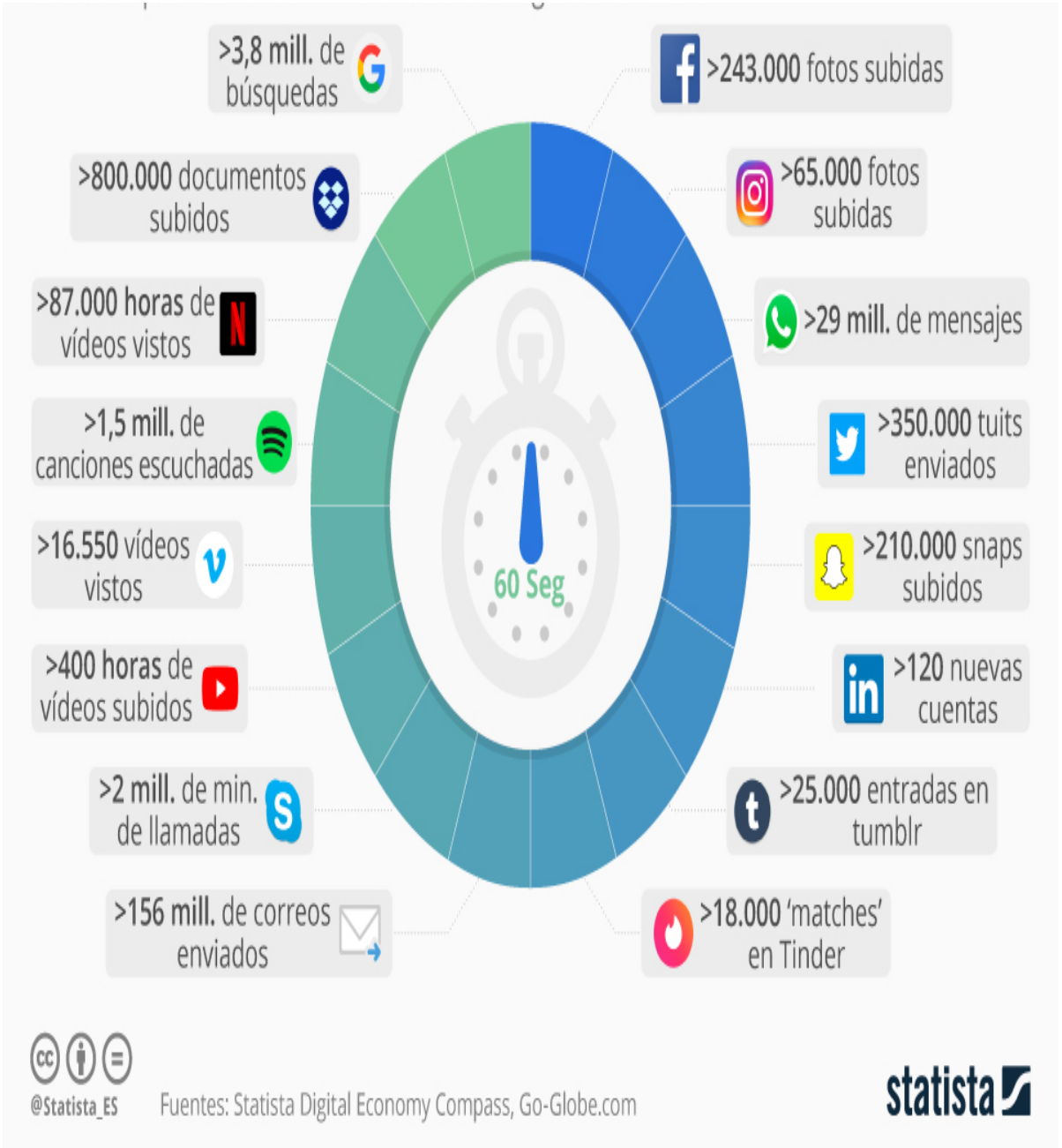
JOHN JAIRO ECHEVERRY ARISTIZABAL
Ingeniero de Sistemas
Especialista en Telecomunicaciones
Master en Auditoría, Seguridad Gobierno y Derecho de las TICs
Celular 3142495534
johnjairo@dphir.co
johnjeche@yahoo.es
John.echeverry@usa.edu.co
John.echeverry@javeriana.edu.co

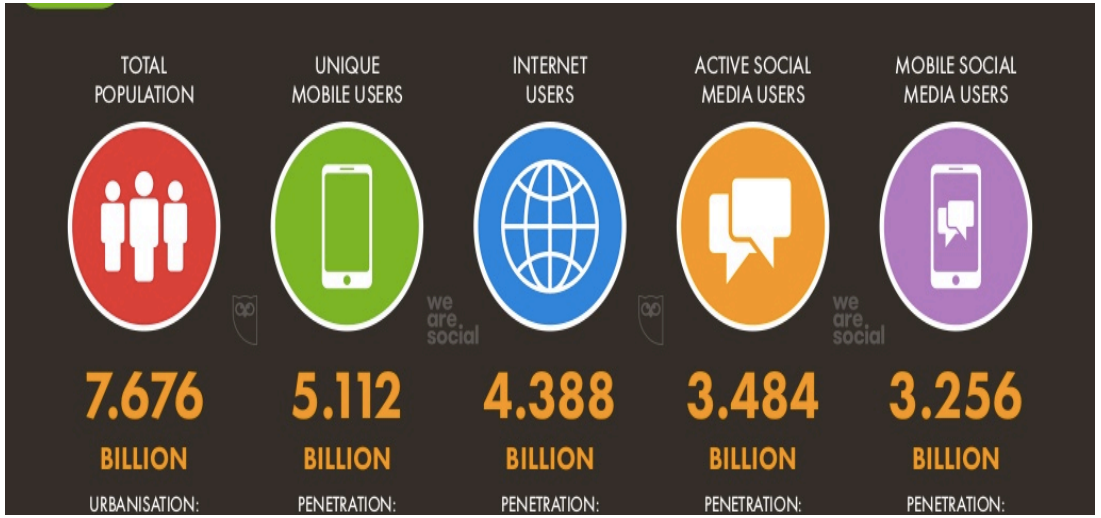
Centro Cibernético Policial

Holística del Cibercrimen en Colombia y Capacidades

CT JULIAN CELY
3232733411

HOLÍSTICA CYBER– DIAGNÓSTICO DE LA PROBLEMÁTICA





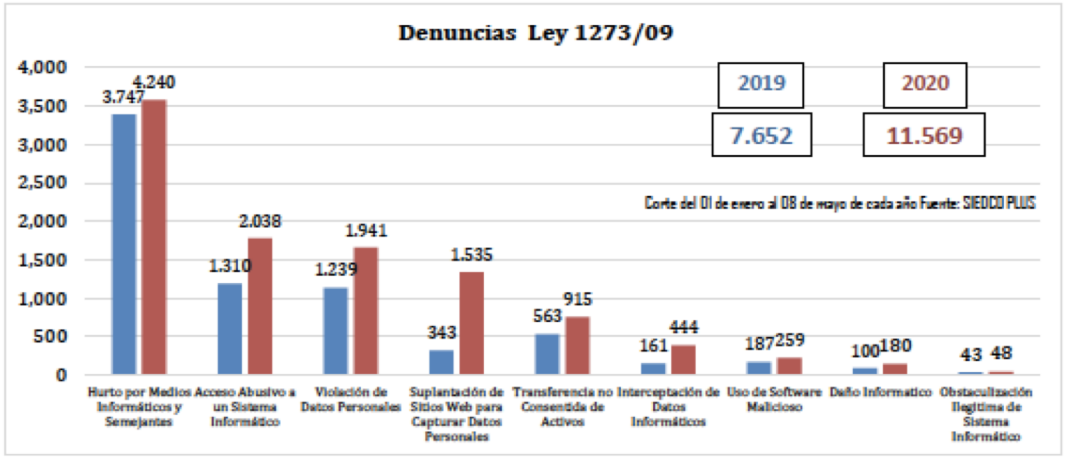
BALANCE CIBERCRIMEN 2020

CENTRO CIBERNÉTICO POLICIAL "CECIP"

Bogotá
Mayo de 2020

Durante el año **2020,** se han presentado diferentes eventos de carácter nacional e internacional que han puesto a prueba la ciberseguridad de la región, los más importantes sin duda hacen referencia a las jornadas de **PROTESTA SOCIAL** y la propagación de la pandemia del **COVID-19.**

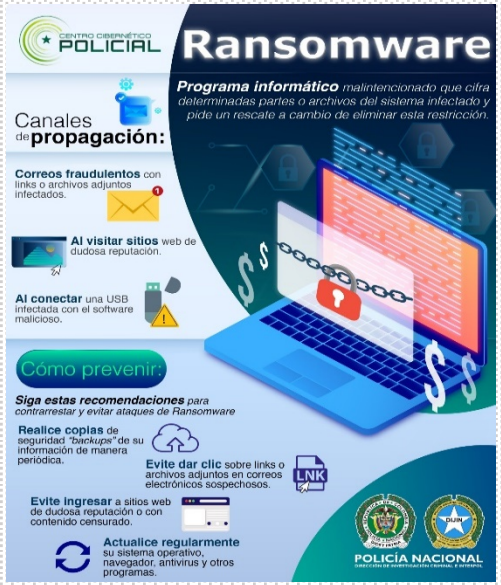
Lo anterior, ha demandado un exponencial incremente en el uso de la Internet y de las tecnologías de la información y las comunicaciones, abriendo con ello una ventana gigantesca de oportunidades para que los ciberdelincuentes ataquen.



Durante el presente año la fluctuación delictiva ha marcado las siguientes tendencias:

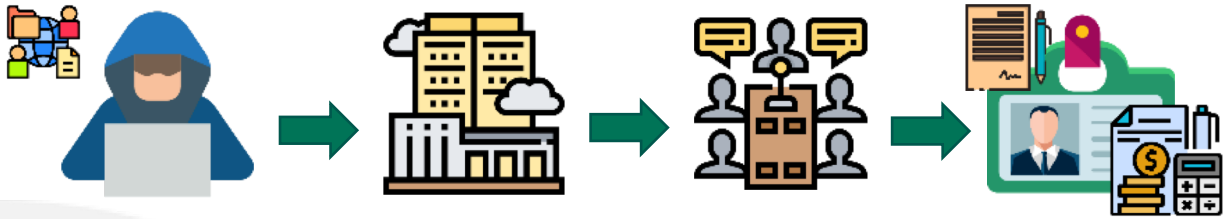
- **46%** de incremento en **DENUNCIAS** por **delitos informáticos** del 01 de enero al 08 de mayo del presente año, comparado con el año anterior. **3.917** casos más.
- **348%** de incremento en la **suplantación de sitios web**, portales falsos que buscan apoderarse de información personal, principalmente bancaria. **1.192** casos más.
- **176%** de incremento en el delito de **interceptación de datos informáticos.**
- **80%** de incremento en el delito de **daño informático.**
- **63%** de incremento en el delito de **transferencia no consentida de activos.**
- **57%** de incremento en el delito de **violación de datos personales.**
- **56%** de incremento en el delito de **acceso abusivo a un sistema informático.**
- **13%** de incremento en el delito de **hurto por medios informáticos y semejantes**

HOLÍSTICA DE VECTORES DE ATAQUE REPORTADOS



FASE 1

SECUENCIA DE ATAQUE: SEMÁNTICO Y SINTÁCTICO



FASE 2

PERFILACIÓN DE VÍCTIMAS Y ELABORACIÓN DE HERRAMIENTAS PARA EL CIBERATAQUE

FASE 3

PRINCIPALES VECTORES DE ATAQUE

RANSOMWARE

TROYANO

DDoS

PHISHING

B.E.C.

CENTRO DE CAPACIDADES PARA LA CIBERSEGURIDAD DE COLOMBIA

Inauguración en agosto del 2018 se el Centro de Capacidades Para la Ciberseguridad de Colombia "C4"

Prevención en la Web

- **Boletines** de últimas tendencias en cibercrimen
- **Guías** de Ciberseguridad, Cartillas
- **Chat CAI Virtual – Atención de Incidentes**

https://caivirtual.policia.gov.co/ *visitas a nuestro portal de servicios* **169.028**

Nuevos seguidores en redes sociales

1.880

Alertas preventivas en redes sociales 2019: **170**

Canal Directo Para el Bloqueo de Portales Web vinculados al abuso sexual de Niños en Internet

2,489 páginas bloqueadas

Ciber Investigación

Ley 1273/09

- **Enlace Directo**

FISCALIA GENERAL DE LA NACION · EUROPOL · INTERPOL

- **Apoyo en Investigaciones** contra Hurto, Fraude Informático, Secuestro de información (***Alcaldías y Gobernaciones son la Mayor Afectación***)
- **Apoyo para Solicitudes de Emergencia** → **Seguridad Ciudadana En Internet**

Amenazas – Extorsión

twitter · facebook · Google · mercado libre

09 LABORATORIOS INFORMÁTICA FORENSE COLOMBIA

Informática Forense

Elementos analizados

986 Dispositivos

GB **Analizadas**

30.524

Muestras analizadas por la plataforma "Daedalus"

418 entre dispositivos móviles y dispositivos de almacenamiento de datos

Estrategia Integral de Ciberseguridad

"Unidades de Investigaciones Tecnológicas"

Reporte de Denuncias

Fuente Siedco

2017 → 15.942

2018 → 21.687

36 %

"El Hurto por Medios Informáticos" fue el delito de mayor afectación en el año 2018-2019.

Hasta **60 Delitos Informáticos Diarios** se denuncian en Colombia.

Top Ciudades

1 Bogotá
2 Medellín
3 Cali
4 Bucaramanga
5 Barranquilla

ESTRATEGIA INTEGRAL DE CIBERSEGURIDAD

DESPLIEGUE ESTRATEGIA INTEGRAL DE CIBERSEGURIDAD (ESCIB)

1 Prevención

- Cuadrante Virtual.
- Análisis fuentes abiertas/Ciberpatrullaje.
- Sistema Gestión de incidentes.
- Denuncia virtual (FGN).
- Difusión de alertas.
- Prevención delitos informáticos.
- Informes de Cibercrimen.
- Ciudadanos impactados/nivel de penetración: (incremento satisfacción).

Actores

INSTITUCIONALES
- **DISEC**
- **DINAE**
- **DIPRO**
- **COEST**
- **ASUIN**
- **INSGE**
- **DIPOL**

*Mesas de Integración.
*Boletín semanal cibercrimen.
*Unificación de procedimientos.
*Creación Manual de Doctrina.
*Difusión ESCIB.
*Ampliación cobertura.

2 Policía judicial / judicialización

- Eje temático del cibercrimen
- Ciberseguridad.
- Economía digital.
- Convivencia Ciudadana Ciberespacio.

Grupos de trabajo:
- Contra el fraude en internet.
- Contra el abuso de las criptomonedas.
- Contra el material de abuso infantil.
- Protección institucional.

- Desarticulación organizaciones criminales.
- Acción efectiva Operacional- mejora tiempos de respuesta.
- Plan reducción cibercrimen.

3 Articulación - cooperación

Presidencia – FGN - Min TIC's

- Mesas de integración (Presidencia).
- Presencia Policía Nacional contexto internacional.
- Ley de ciberseguridad.
- Implementación grupos de trabajo, fuerzas de tarea cibernética.
- Atención de amenazas.
- Análisis criminales.
- Desarrollo de convenios y alianzas.

Min TIC's - PONAL
- Intercambio de Información.
- Articulación institucional.

Centro de Capacidades para la Ciberseguridad de Colombia. C4

FISCALIA GENERAL DE LA NACIÓN · UIAF · CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO · Superintendencia Financiera de Colombia · ASOBANCARIA · INCOCREDITO · CCIT · Industria y Comercio Superintendencia · EC3 EUROPOL · UNODC

PLATAFORMAS EN CIBERSEGURIDAD

CENTRO CIBERNÉTICO POLICIAL

EUROPOL SIENA

LEY 1582/12

Plataforma EMAS EUROPOL

Law Enforcement Enterprise Portal (LEEP) FBI

Herramienta de búsqueda de información **EN FUENTES ABIERTAS**

Plataforma web segura y colaborativa para ***especialistas en Ciberseguridad***

Instrumento de **intercambio de información** ***NNA*** Abuso sexual en N.N.A

Punto Oficial del D.O.J ***Para la red de Cibercrimen***

COLOMBIACHECK - No coma cuento -

NO MORE RANSOM!

CSIRT Sectoriales

* **Gobierno**
* **Financiero**

SIENA (Secure **Information Exchange Network** Application) **Canal de comunicación seguro**

Plataforma EMAS (European **Malware Analysis** Solution), Sistema de análisis de Malware

Herramientas de investigación basadas en la web y recursos analíticos EE.UU.

CANAL OFICIAL Enlace Seguro Coordinación Con **Redes Sociales**

LEY 1928/18

Búsqueda de información en fuentes abiertas - Ciberpatrullaje

EUROPOL EC3 European Cybercrime Centre EPE

ICSE International Child Sexual Exploitation Database INTERPOL

G8 24-7 High Tech Crime Network

24/7 CONVENIO DE BUDAPEST

TRANSVERSAL

CAPACIDADES EN INFORMÁTICA FORENSE

- BIG DATA
- 1er Lab. Malware
- UFED 4PC
- NUIX – AXIOM

BLOQUEO DE CONTENIDOS

MEJORES PRÁCTICAS : CIBERESILENCIA ORGANIZACIONAL

Identificar	Proteger	Detectar	Responder	Recuperar
Gestión de activos	Control de acceso	Anomalías y eventos	Respuestas	Recuperación
Entorno empresarial	Concienciación y formación	Control continuo de la seguridad	Planificación	Planificación
Dirección	Seguridad de los datos	Procesos de detección	Comunicaciones	Mejoras
Evaluación de riesgos	Procesos y procedimientos de protección de la información		Análisis	Comunicaciones
Estrategia de la evaluación de riesgos	Mantenimiento		Mitigación	
Gestión de riesgos de la cadena de suministro	Tecnología de protección		Mejoras	

La resiliencia es la capacidad que tiene un sistema para prepararse, anticipar, adaptarse, continuar trabajando o recuperar su funcionamiento, cuando su normal operación ha sido alterada.

EL ÚNICO FIN ES GARANTIZAR LA DISPONIBILIDAD, INTEGRIDAD , CONFIDENCIALIDAD Y NO REPUDIO DE LA INFORMACION DE UNA PYME NO IMPORTA SU ESCALA

Sistema de Gestión de Seguridad de la Información

Resolución 08310 de 26 Diciembre de 2016

Política

La Policía Nacional de Colombia se compromete a salvaguardar sus activos de información con el fin de protegerlos de las amenazas que se ciernen sobre ellos, a través de la implementación de un Sistema de Gestión de Seguridad de la Información que permita la adecuada gestión del riesgo, la generación de estrategias de seguridad basada en las mejores prácticas y controles, el cumplimiento de los requisitos legales, la oportuna gestión de los incidentes, y el compromiso Institucional de mejora continua.

Alcance

"La Dirección de Investigación Criminal e INTERPOL, mantendrá el Sistema de Gestión de Seguridad de la Información en el Proceso Desarrollar Investigación Judicial y en el Área Administrar Informar Criminal, orientados a proteger sus activos, mediante la gestión de riesgos, con el fin de garantizar la disponibilidad, confidencialidad e Integridad de la Información, así mismo para los procesos de Desarrollar Investigación Criminalística y Desarrollar Investigación Criminológica, contaran con los controles establecidos por la oficina de Telemática de la Policía Nacional, generando cultura basadas en buenas prácticas".

DIJIN

SGSI

Objetivos

- Crear una cultura de seguridad de la información en cada unidad policial, mediante sensibilizaciones y capacitación en cuanto a las mejores prácticas para evitar la materialización de riesgos asociados al **SGSI**.
- Identificación mediante una adecuada evaluación del riesgo, el valor de la información, así como las vulnerabilidades y las amenazas a las que están expuestas.
- Dar un tratamiento efectivo a los incidentes de seguridad, con el fin de identificar sus causas y realizar las acciones correctivas.

- Implementar y mantener el Sistema de Gestión de Seguridad de la Información promoviendo la mejora continua.

Responsabilidades con el SGSI

1.Clasificación de la Información. Clasificar la información

2.Parágrafo de la Reserva. Informar oportunamente novedades

3.Buenas practicas- Apagar equipos de computo

4.Partes Interesadas. Contraseñas seguras

Utilizar equipos autorizados

Cumplir controles seguridad instalaciones

Guardar bajo llave documentos impresos

Escritorios y pantallas limpias

Evitar e informar anomalías

Almacenar la información en las carpetas corresponde

Firmar acuerdos de confidencialidad

No prestar el usuario

Bloquear la sesión cuando se levante del puesto de trabajo

No utilizar dispositivos no autorizados (usb, tablets, etc.)

Acceder a las carpetas autorizadas

Proteger la información institucional

Activos de Información

DEPENDENCIA	TIPO DE ACTIVO	DESCRIPCIÓN
CECIP	Hardware	Equipos de Computo
	Hardware	Computador portátil
	Infraestructura	Sala C-4
	Hardware	Sistema de conferencia CISCO
	Hardware	Pantallas video ball
	Infraestructura	Cuarto de equipos
	Información física	Archivos de gestión
	Servicio	Portal Caí Virtual
	Hardware	Estaciones forenses
	Hardware	Servidor applance nutanix
	Hardware	Switch dell
	Hardware	Equipo TX1
	Hardware	UFED Cellebrite
	Software	UFED Cellebrite 4PC
	Hardware	Kit bloqueador forense con TD3
	Hardware	Licencia de Encase
	Software	Encase forensic
	Hardware	Licencia Internet Evidence Finder
	Software	Programa IEF
	Software	Licencia arbutus
	Hardware	Herramienta de Borrado Seguro
	Hardware	Licencia Blade
	Software	Programa Blade
	Información electrónica	Peritajes forenses
	Información electrónica	Carpetas compartidas
	Infraestructura	Laboratorio de informática forense
	Servicio	Sistemas de Información

RECOMENDACIONES -CIBERSEGURIDAD

INFORMAR AL CAIVIRTUAL PARA RESOLVER INQUIETUDES

EVITE CONECTARSE A REDES PÚBLICAS Y GRATUITAS.

PONER EN PRÁCTICA LA EDUCACIÓN Y LA SENSIBILIZACIÓN DE LOS USUARIOS

MANTENER LOS SISTEMAS AL DÍA

TENER CUIDADO AL DESCARGAR ARCHIVOS ADJUNTOS EN CORREOS E.

APLICAR SEGURIDAD DE DISPOSITIVOS MÓVILES

NO INGRESAR A LA BANCA VIRTUAL A TRAVÉS DE LINK EN CORREOS

VERIFIQUE CAMBIOS EN PAGOS DEL PROVEEDOR Y CONFÍRMELOS.

DESCONFÍE DE LAS SOLICITUDES DE PAGO QUE PIDAN UNA ACTUACIÓN URGENTE.

REALICE BUENAS PRÁCTICAS DE CLOUD CLOUTHING

IMPLEMENTAR HARDWARE Y SOFTWARE PARA FORTALECER LA SEGURIDAD

UTILIZAR CONTRASEÑAS SEGURAS Y MANTENERLAS SEGURAS

REALIZAR Y REVISAR COPIAS DE SEGURIDAD DE LOS DATOS DE NEGOCIO E INFORMACIÓN

NO BRINDAR INFORMACIÓN FINANCIERA A TRAVÉS DE LLAMADAS TELEFÓNICAS

CREE REGLAS DE DETECCIÓN DE INTRUSOS QUE ALERTEN SOBRE EMAILS FRAUDULENTOS

NO PUBLIQUE INFORMACIÓN FINANCIERA EN REDES SOCIALES.

CONOZCA LOS HÁBITOS DE SUS CLIENTES Y SUS PAGOS

2020 TENDENCIAS 2020

En 2020 el Cibercrimen seguirá sofisticando su actuar delictivo y utilizará las capacidades tecnológicas disponibles a su favor.

Inteligencia Artificial y Malware

El escaneo automatizado de vulnerabilidades por parte de los Cibercriminales facilitará la detección de víctimas potenciales. El Malware podrá detectar si un sistema de seguridad le está analizando (sandbox) y se auto eliminará.

Lo anterior supone un desafío adicional para los investigadores, porque estas técnicas antiforenses eliminarán evidencia digital en los equipos y sistemas infectados de empresas y ciudadanos víctimas.

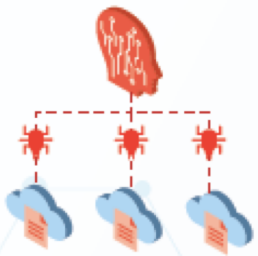
Uso de perfiles falsos en redes sociales para difusión de Malware

Cuentas falsas en redes sociales como Twitter y Facebook serán usadas para generar contenidos de manera automatizada masificando las cifras de infección de malware.

BEC basado en Deepfake

Las empresas en Colombia podrán recibir audios e incluso videos, en los cuales los cibercriminales suplanten a ejecutivos, clientes y proveedores para conseguir transferencias de dinero o despacho de productos.

La tecnología Deepfake es una técnica basada en Inteligencia Artificial, que coloca imágenes o videos sobre otro video, así como imitación de voces.



Uso de Botnet para difusión de correos extorsivos

Se prevé el incremento de casos de Sextorsión, basados en el envío masivo de mensajes por parte de los cibercriminales utilizando equipos controlados remotamente (Botnet). La tasa podrá alcanzar hasta 30 mil correos por hora.

Uso de mercados ilegales en DarkNet

El cibercrimen seguirá utilizando los foros de la Dark-Net para la venta de datos bancarios en la internet Profunda. Aprovecharán el creciente uso de Criptomonedas en Colombia para facilitar la dispersión de las ganancias de los Ciberataques.

Contacténos

@caivirtual

caivirtual

Cai Virtual

https://caivirtual.policia.gov.co/

GRACIAS