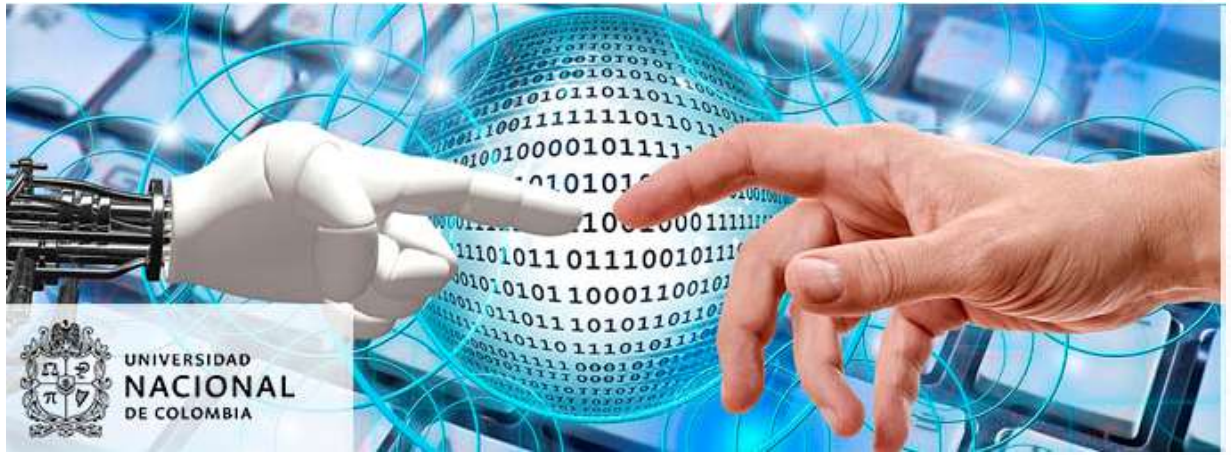
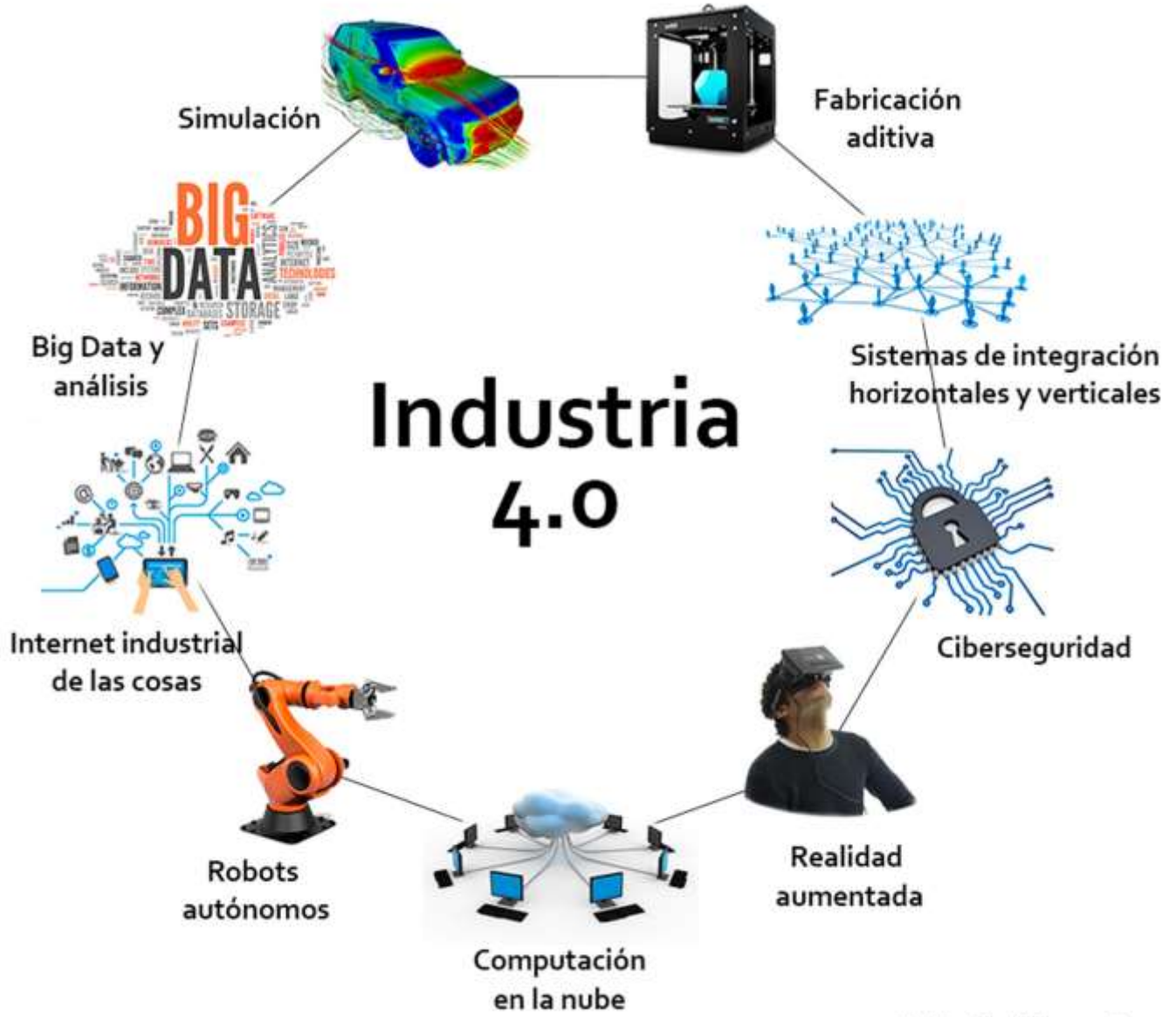


Ciberseguridad

Francisco Javier Valencia Duque
PhD en Ingeniería, Industria y Organizaciones
Director Grupo de Investigación en Teoría y Gestión de Tecnologías de Información.
Universidad Nacional de Colombia
fjvalenciad@unal.edu.co

Los pilares de la industria 4.0



Que es ciberseguridad

ITU-T X.1205:2008

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el **ciberentorno**. Las propiedades de seguridad incluyen uno o más de las siguientes: disponibilidad, integridad (que puede incluir autenticidad y el no repudio) y confidencialidad(ITU, 2008, p.3).

ISACA

Protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se **encuentran interconectados**.

ISO/IEC 27032:2012

preservación de la confidencialidad, integridad y disponibilidad de la información en el **ciberespacio**, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, software y servicios en Internet, a través de **dispositivos tecnológicos y redes conectadas** a él, que no existen en ninguna forma física

Diferencias entre seguridad de la información, seguridad informática y ciberseguridad

Seguridad de la Información

El sistema de gestión de seguridad de la información preserva la Confidencialidad, Integridad y Disponibilidad de la Información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente. (ISO/IEC 27001:2013)

Seguridad Informática

De acuerdo con Cano(2011) la seguridad informática o seguridad de TI es la función táctica y operacional de la seguridad, la que se encarga de las implementaciones técnicas de la protección de la información, de las tecnologías antivirus, firewalls, IDS, manejo de incidentes

Ciberseguridad

ISACA (2016) la define como la protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se ***encuentran interconectados***.

¿Diferencias sustanciales entre seguridad informática, seguridad de la información y Ciberseguridad

La diferencia entre los términos genéricos seguridad informática y seguridad de la información, se da ***en función del tipo de recursos*** sobre los que actúa, mientras que ***la primera se enfoca en la tecnología propiamente dicha***, en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, ***la segunda está relacionada con la información, como activo estratégico de la organización***. En este sentido las TIC son herramientas que permiten optimizar los procesos de gestión de la información en las organizaciones. Y la ciberseguridad **esta asociada al ciberespacio y a la infraestructura que la soporta.**

Principales referentes de ciberseguridad a nivel internacional

ISO/IEC TR 27103:2018	*Tecnología de información- Técnicas de seguridad- ciberseguridad y estándares ISO/IEC*	2018
NIST Cibersecurity Framework	*Marco de referencia para el mejoramiento de la ciberseguridad de infraestructuras críticas.*	2018
SANS	Controles críticos de ciberseguridady su relación con el marco de referencia de ciberseguridad del NIST	2018
Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de la Unión Europea	Directiva Europea de Ciberseguridad	2016
Orden Ejecutiva (OE 13636) USA	*Mejorando la ciberseguridad de las infraestructuras críticas*	2013
ISO/IEC 27032	Cubre aspectos no contemplados en las normas de seguridad de la información, y elementos de comunicación entre las organizaciones y los proveedores en el ciberespacio	2012
UIT-T X.1205 de 2008	*Aspectos generales de la ciberseguridad*	2008
Convenio de Budapest	Convenio sobre la ciberdelincuencia	2001

¿Principios y aspectos estructurales de la ciberseguridad

Principios

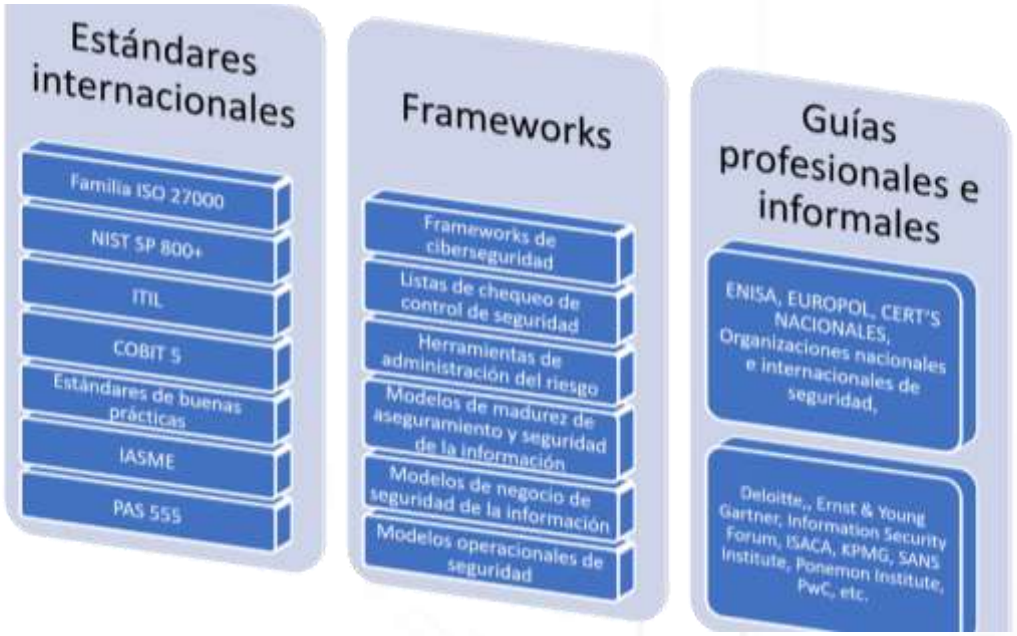
Confidencialidad
Integridad
Disponibilidad

Capas Tecnológicas

1	PROCESOS DE NEGOCIO	BAAS
2	SERVICIOS DE TI	
3	DATOS/INFORMACIÓN/CONOCIMIENTO	
4	SISTEMAS DE INFORMACIÓN TRANSACCIONALES	SAAS
5	SISTEMAS DE INFORMACIÓN SOPORTE	
6	MOTORES DE BASES DE DATOS	PAAS
7	SISTEMAS OPERATIVOS	
8	PC's DE ESCRITORIO E IMPRESORAS	IAAS
9	SERVIDORES (Físicos, virtuales y en la nube)	
10	CENTROS DE REDES Y CABLEADO	
11	CENTROS DE COMPUTO	
12	ENERGIA	

Fuente: (Valencia Duque, Marulanda, & López Trujillo, 2015)

Estándares seguridad de la información



Fuente: (Valencia Duque, 2018)

¿Principios y aspectos estructurales de la ciberseguridad

ISO/IEC 27002:2013

Prácticas de control de SGSI

Categorías de procesos del marco de referencia de ciberseguridad del NIST.

Controles de seguridad críticos (versión 6.0.)

(Centro de Seguridad de Internet – SANS-)

ISO/IEC 27032:2012

ISO/IEC TR 27103:2018

ISO/IEC 27001:2013

Taxonomias

+

ISO/IEC 27005:2008

Gestión del riesgo de un SGSI

ISO/IEC 27003:2010

Guía de implementación de un SGSI

Fuente: (Valencia Duque, Marulanda, & López Trujillo, 2015)

¿Principios y aspectos estructurales de la ciberseguridad

Categorías de procesos del marco de referencia de ciberseguridad del NIST.

Funciones	Categorías	
Identificar	AM	Gestión de activos
	BE	Ambiente de negocios
	GV	Gobierno
	RA	Evaluación de riesgos
	RM	Estrategia de gestión del riesgo
	SC	Gestión del riesgo de la cadena de suministro
Proteger	AC	Gestión de identidad y control de acceso
	AT	Concientización y capacitación
	DS	Seguridad de datos
	IP	Procesos y procedimientos de protección de información
	MA	Mantenimiento
	PT	Protección de tecnología
Detectar	AE	Anomalías y eventos
	CM	Monitoreo continuo de la seguridad
	DP	Procesos de detección
Responder	RP	Planeación de la respuesta
	CO	Comunicación
	AN	Análisis
	MI	Mitigación
	IM	Mejoras
Recuperar	RP	Planeación de la recuperación
	IM	Mejoras
	CO	Comunicación

Controles de seguridad críticos (versión 6.0.) (Centro de Seguridad de Internet – SANS-)		Marco de referencia de ciberseguridad del NIST				
		Identificar	Proteger	Detectar	Responder	Recuperar
1	Inventario de dispositivos autorizados y no autorizados	AM				
2	Inventario de software autorizado y no autorizado	AM				
3	Configuración segura de dispositivos de usuario final		IP			
4	Evaluación continua de vulnerabilidades & remediación	RA		CM	MI	
5	Uso controlado de privilegios administrativos		AC			
6	Monitoreo, mantenimiento y análisis de logs de auditoría			AE	AN	
7	Protección de e-mail y browsers		PT			
8	Defensa de malware		PT	CM		
9	Limitación y control de puertos de red, protocolos y servicios		IP			
10	Capacidad de recuperación de datos					RP
11	Configuración segura de dispositivos de red		IP			
12	Defensa perimetral			DP		
13	Protección de datos		DS			
14	Acceso controlado basado en la necesidad de conocer		AC			
15	Control de acceso inalámbrica		AC			
16	Monitoreo y control de cuentas		AC	CM		
17	Evaluación de habilidades de seguridad y entrenamiento apropiado		AT			
18	Seguridad de aplicaciones de software		IP			
19	Administración y respuesta a incidentes			AE	RP	
20	Test de penetración y ejercicio de equipos rojos				IM	IM

Como se están preparando las organizaciones para hacer frente a la ciberseguridad

Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
TOTAL	**5797**	**7732**	**9246**	**12935**	**15626**	**17355**	**19620**	**21604**	**23005**	**27536**	**33290**	**39501**
Africa	6	10	16	47	46	40	64	99	79	129	224	301
Central / South America	18	38	72	100	117	150	203	272	273	347	564	620
North America	79	112	212	322	329	435	552	712	814	1445	1469	2108
Europe	1064	1432	2172	3563	4800	5289	6379	7952	8663	10446	12532	14605
East Asia and Pacific	4210	5550	5807	7394	8788	9665	10422	10116	10414	11994	14704	17562
Central and South Asia	383	519	839	1303	1328	1497	1668	2002	2251	2569	2987	3382
Middle East	37	71	128	206	218	279	332	451	511	606	810	923

Fuente: elaborado a partir de (ISO, 2018)

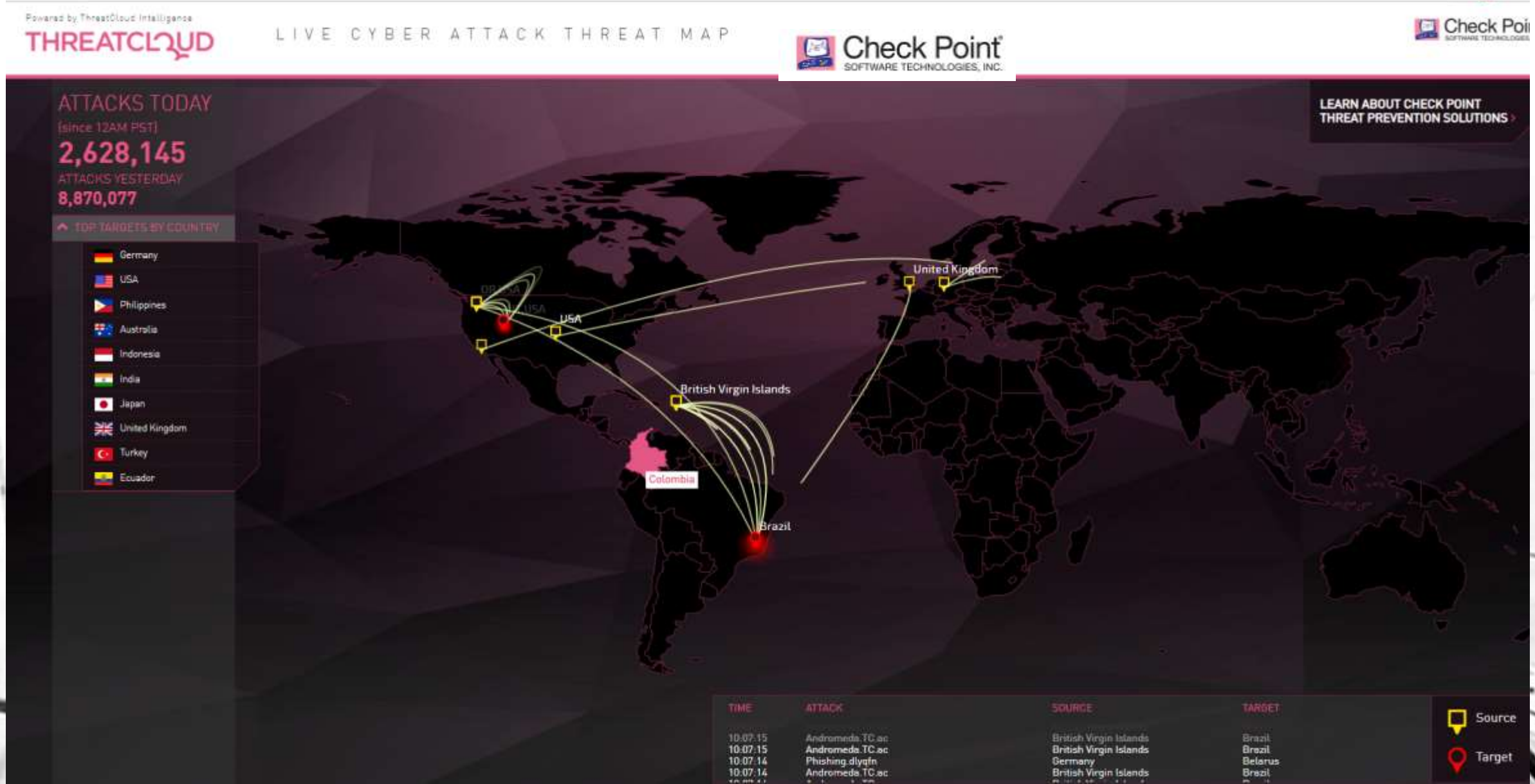
Incremento de aproximadamente 581% en los últimos 10 años

Colombia 3 8 11 14 23 27 58 82 78 103 163 148

¿Monitoreo en línea de la ciberseguridad a nivel internacional

¿Monitoreo en línea de la ciberseguridad a nivel internacional

¿Monitoreo en línea de la ciberseguridad a nivel internacional



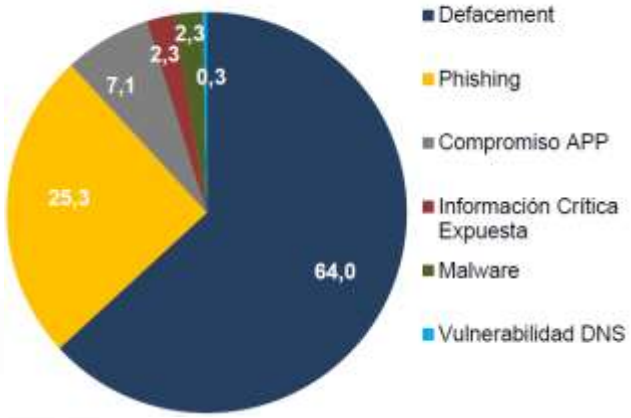
Decálogos de Ciberseguridad

	CENTRO CRIPTOLÓGICO NACIONAL DE ESPAÑA	INCIBE	FUNDACIÓN INNOVACIÓN BANKINTER
1	Aumentar la capacidad de vigilancia de las redes y los sistemas. Es indispensable contar con el adecuado equipo de ciberseguridad	Políticas y normativas que van a dirigir la forma de abordar la seguridad en el día a día.	Reducir los costos globales de ciberataques y cibercrimen a través de la colaboración conjunta de los paises
2	Monitorización y correlación de eventos. Uso de herramientas capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etc	Control de accesos lógicos	Garantizar la integridad de las infraestructuras y soluciones tecnológicas
3	Política de Seguridad Corporativa restrictiva. Adecuación progresiva de los permisos de usuario, servicios en la "nube" y la utilización de dispositivos y equipos propiedad del usuario (BYOD)	Copias de seguridad	Extender el uso de la tecnología de autenticación de doble factor
4	Configuraciones de seguridad en todos los componentes de la red corporativa. Se incluirán los dispositivos móviles y portátiles	Protección antimalware	Educar a los ciudadanos en ciberseguridad
5	Uso de productos, equipos y servicios confiables y certificados. Redes y sistemas acreditados para información sensible o clasificada.	Actualizar todo el software	Concientizar al consumidor digital en seguridad
6	Automatizar e incrementar el intercambio de información. Reciprocidad con otras organizaciones y Equipos de Respuesta a Incidentes de Seguridad de la Información (CERTs)	Seguridad en la red	Proteger los datos nacionales en Internet más allá de las fronteras territoriales
7	Compromiso de la Dirección con la ciberseguridad. Los cargos directivos deben ser los primeros en aceptar que existen riesgos y promover las políticas de seguridad.	Acceso desde el exterior (Información en tránsito)	Responsabilidad penal por el software inseguro
8	Formación y la Sensibilización de usuarios (eslabón más débil de la cadena). Todos y cada uno de los niveles de la organización (dirección, gestión e implantación) deben ser conscientes de los riesgos y actuar en consecuencia	Controlar los soportes	Software de calidad
9	Atenerse a la legislación y buenas prácticas. Adecuación a los distintos estándares (en el caso de las Administraciones Públicas al Esquema Nacional de Seguridad -ENS-)	Registro de actividad	Impulsar una estrategia de ciberseguridad global
10	Trabajar como si se estuviese comprometido. Suponer que los sistemas están ya comprometidos o lo estarán pronto y proteger los activos fundamentales.	Continuidad de negocio	Colaboración público-privada
FUENTE	(CCN-CERT, 2018)	(INCIBE, 2018)	(Joyanes Aguilar, 2017)

Estado actual en Colombia

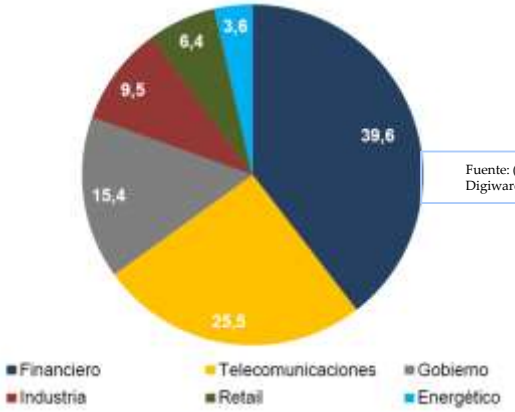
El cibercrimen en el país aumentó 28,3% en 2017 frente a los resultados de 2016 y 446 empresas reportaron haber sido víctimas de ciberataques (Centro cibernético policial, 2017)

Tipos de incidentes cibernéticos en Colombia 2017

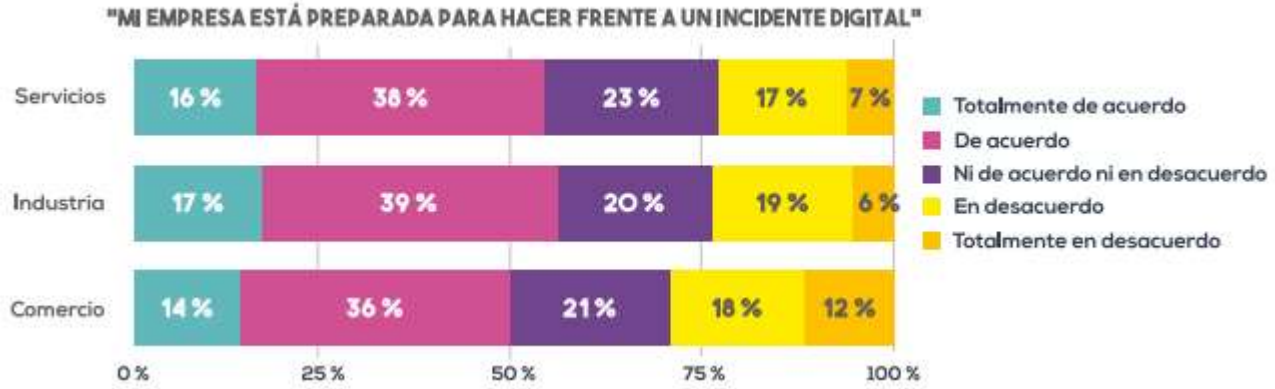


Fuente: (Asobancaria, 2018) basado en COLCER

Distribución de los ataques cibernéticos por sector en 2017



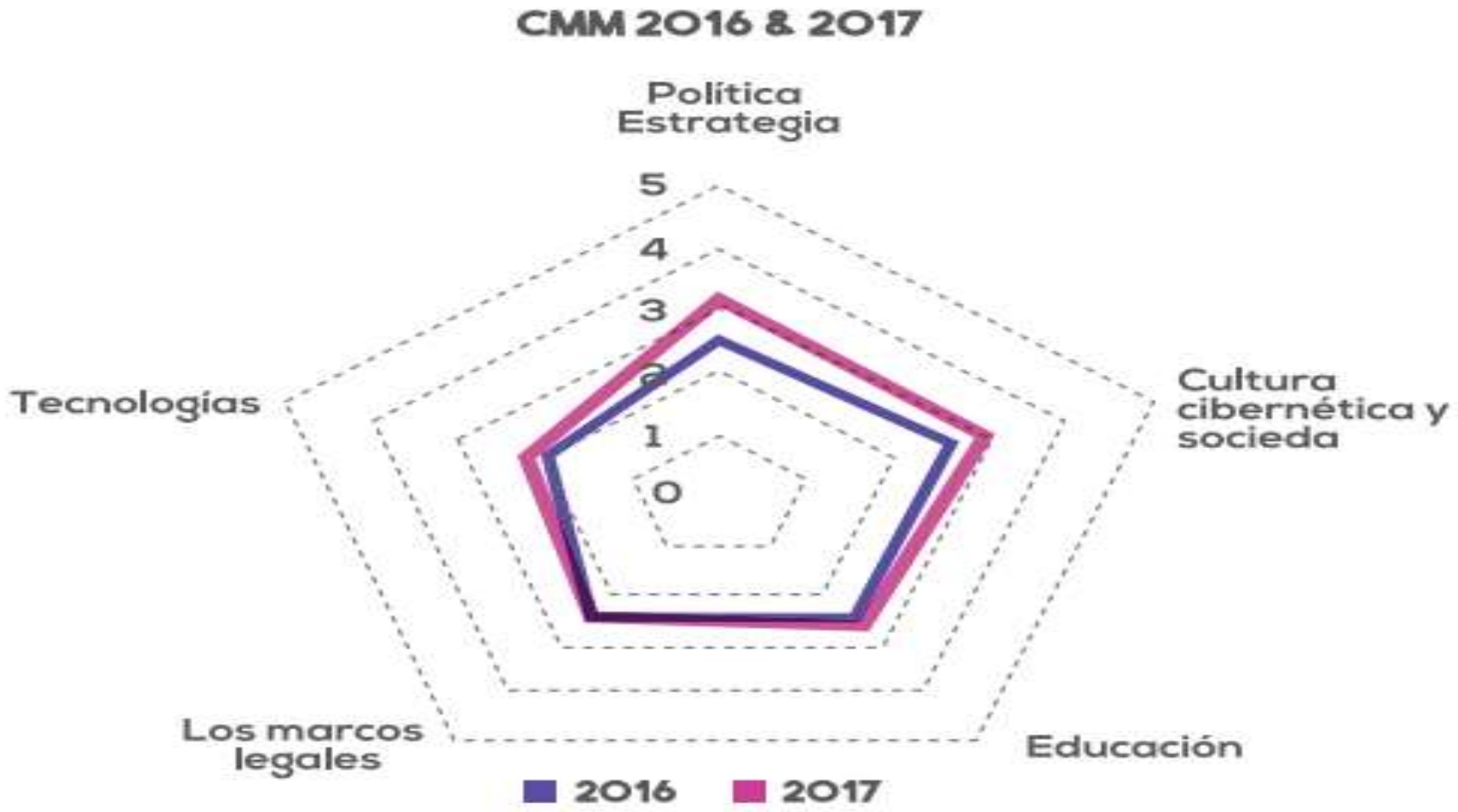
Fuente: (Asobancaria, 2018) basado en Digiware



Fuente: (BID, MINTIC, OEA, 2017)

Defacement: significa desfiguración y es un término usado para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.

Estado actual en Colombia



Fuente: (BID, MINTIC, OEA, 2017)

Estado actual en Colombia (Directrices y estructuras)

Normativo	
Conpes 3701:2011	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Conpes 3854:2016	Política Nacional de Seguridad Digital
Institucional	
Centro Cibernético Policial–CCP	
Colcert(Grupo de Respuesta a Emergencias Cibernéticas de Colombia)	Tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional.
CCOC (Comando conjunto cibernético)	Se desempeña como unidad élite en aspectos relacionados con la Ciberseguridad y Ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales, desarrollando operaciones militares en el ciberespacio
CSIRT-PONAL	Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL
CSIRT-Asobancaria	Equipo de Respuesta a Incidentes de Seguridad en el sector financiero.

Muchas gracias