



Asociación Colombiana
de Ingenieros

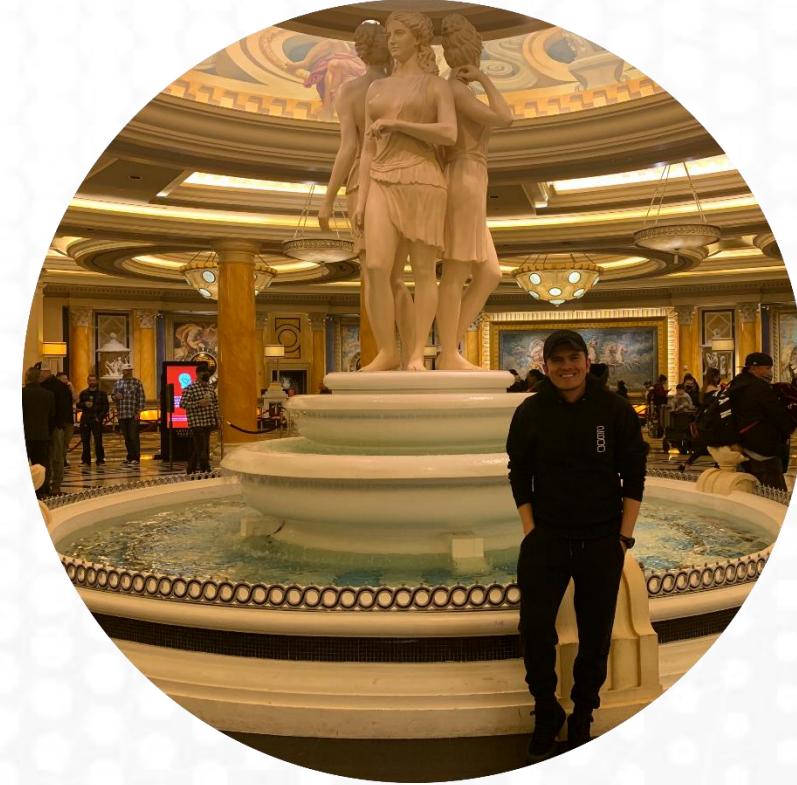
MITOS Y REALIDADES DE LA CIBERSEGURIDAD

(Lecciones aprendidas)

Mayo 16 de 2024

Sobre CHackA0101

Jairo Garcia, conocido como chacka0101, es un Ethical Hacker con más de 20 años de experiencia, máster en seguridad de las TICs, cuenta con múltiples certificaciones de hacking, programador Python, desarrollador de exploits publicados a nivel internacional. Pertenece a la comunidad HOPE (HACKERS OF PLANET EARTH). TOP 14 a nivel mundial de Hack The Box 2021. Experiencia en el sector de OIL & GAS como Ecopetrol, Pacific Rubiales, OCENSA, EQUION, FRONTERA y HOCOL.



<https://www.linkedin.com/in/chacka0101/>



<https://github.com/chacka0101>



¡Descubre
nuestra nueva
plataforma de
intermediación
laboral!"



Temario



CIL

Centro de
Información
Laboral



¡Descubre
nuestra nueva
plataforma de
intermediación
laboral!"



- ✓ Introducción y fundamentos al mundo de la ciberseguridad.
- ✓ El universo de la ciberseguridad.
- ✓ Certificaciones profesionales en el mundo de la ciberseguridad.
- ✓ Cumplimiento normativo de Ciberseguridad (ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)
- ✓ La Ciberseguridad en el mundo corporativo.
- ✓ La Ciberseguridad en el hogar.
- ✓ Retos de Ciberseguridad, Ataques actuales por medio de la AI, entre otros.

¿Qué es la Ciberseguridad?

Introducción y fundamentos al mundo de la ciberseguridad.



<https://www.cimcor.com/blog/the-cia-triad-defining-integrity>

Seguridad Informática

Seguridad de las TICs

Sistemas / TICs

Seguridad de la Información

Es la suma de todas las seguridades para proteger el activo más valioso, la información.

Ciberseguridad Es la evolución de las anteriores.

????????????
Debemos prepararnos para el futuro AI

Además de las seguridad de la información, incluye las infraestructuras críticas.



<https://www.fayerwayer.com/2019/11/infraestructura-critica-chile/>

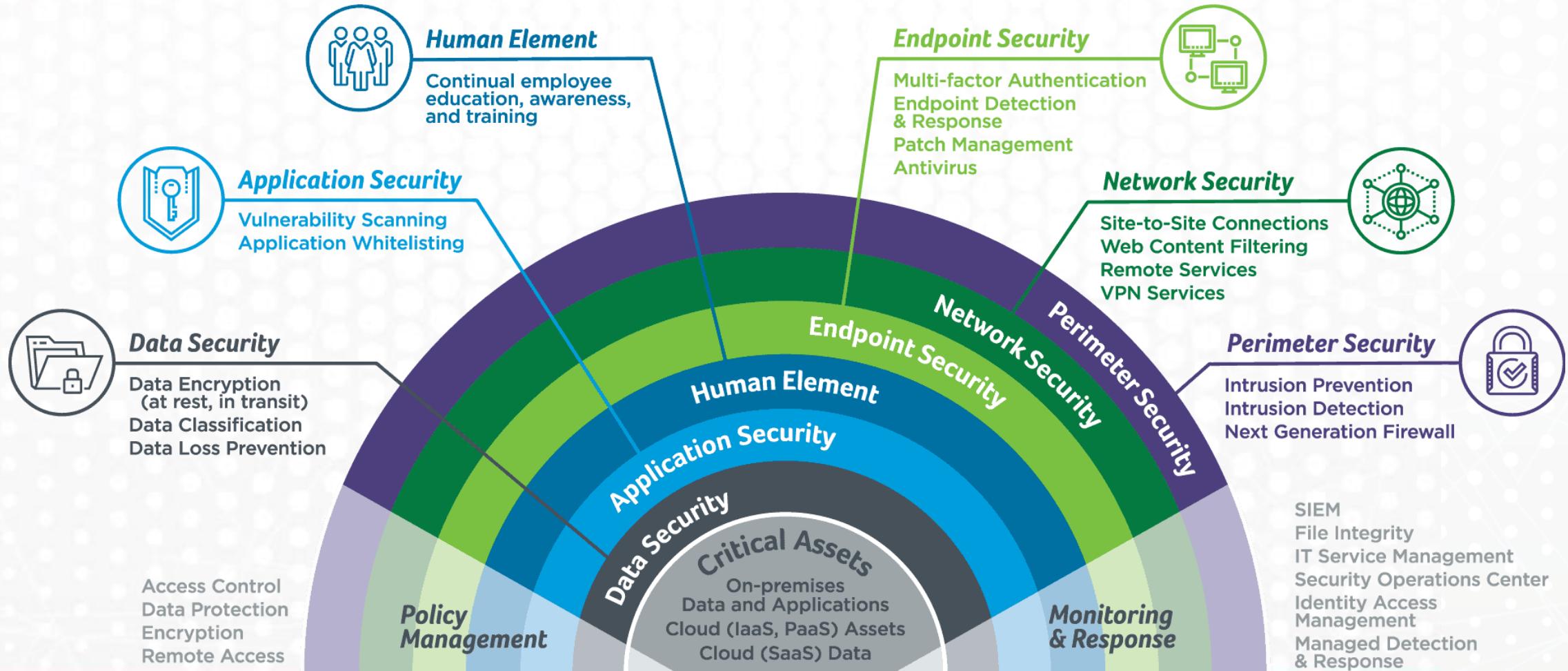
La REALIDAD de la Ciberseguridad es que...

**LO ÚNICO SEGURO EN ESTA VIDA
ES...**



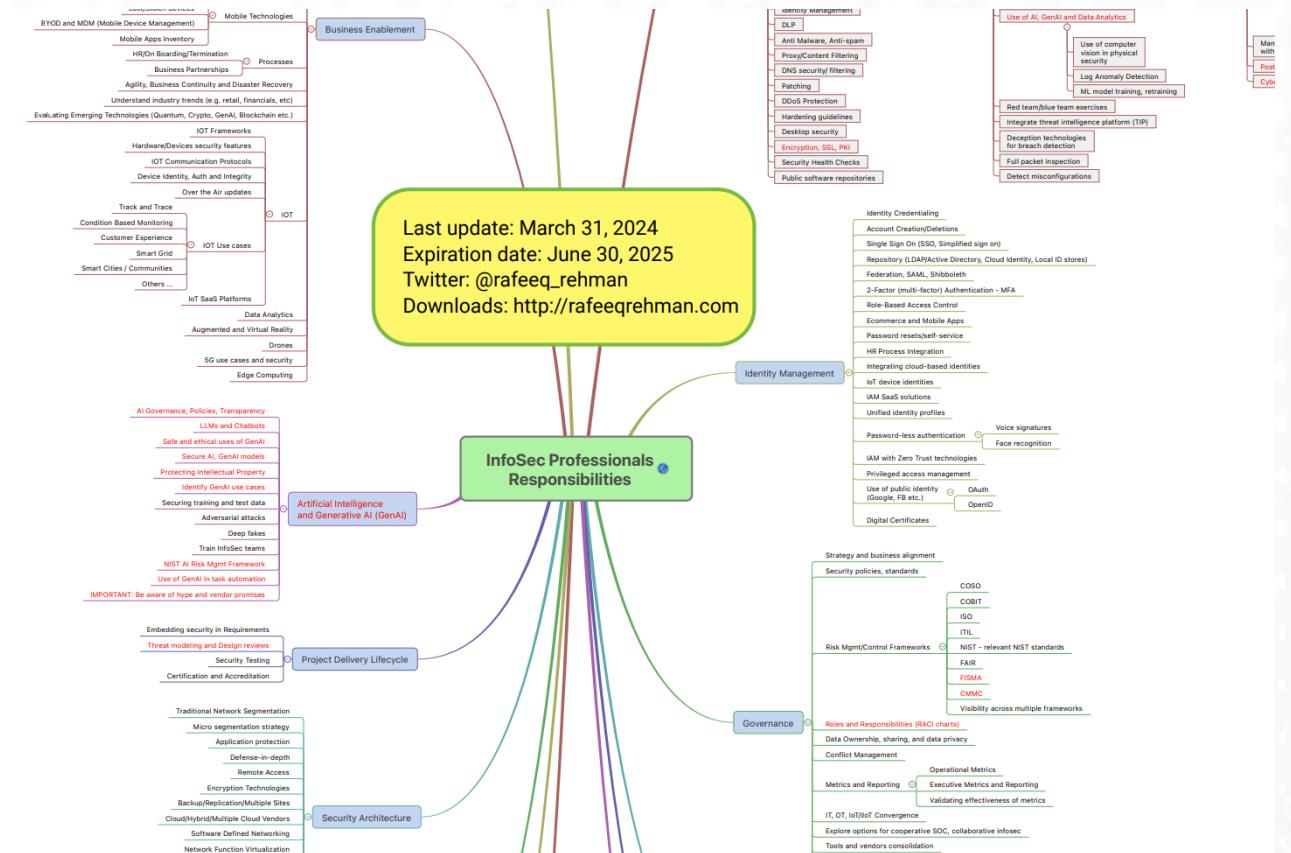
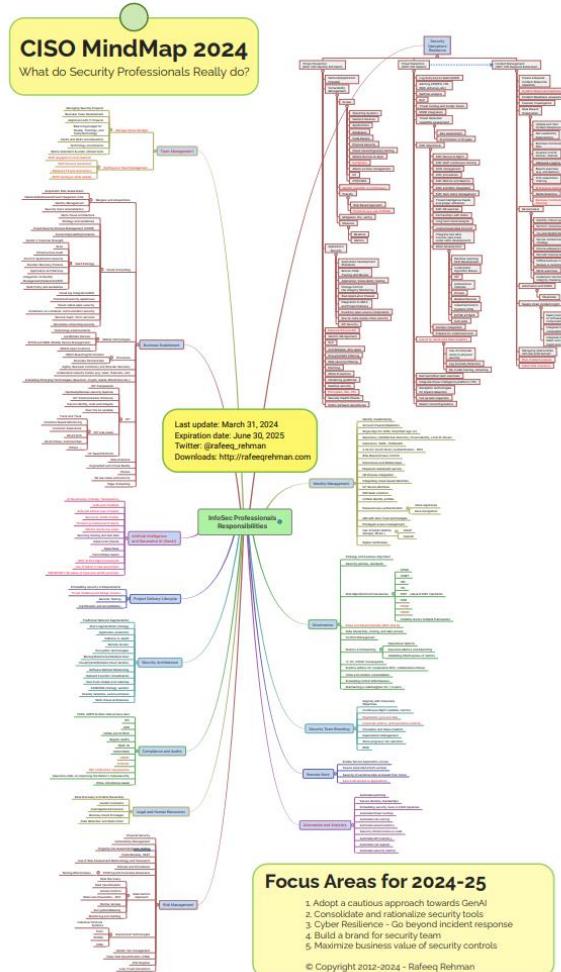
Niveles de la de defensa en profundidad

Introducción y fundamentos al mundo de la ciberseguridad.



Dominios de la Ciberseguridad (Mapa CISO)

El universo de la ciberseguridad.



Dominios de la Ciberseguridad (Mapa CISO)

El universo de la ciberseguridad.



CURRICULUM
Get the right training to build and lead a world-class security team.

FOUNDATIONAL

MGT512 Security Leadership Essentials for Managers

MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep

INT514 SANS Training Program for CISSP Certification GRC

MTR515 A Practical Introduction to Cybersecurity Risk Management

INT516 Security Strategic Planning, Policy, and Governance GRC

SEC566 Implementing and Auditing the Critical Security Controls – In-Depth GRC

MGT516 Managing Security Vulnerabilities: Enterprise and Cloud

SPECIALIZATION

AUD507 Auditing & Monitoring Networks, Perimeters, and Systems GRC

LDS503 Law of Data Security and Investigations GRC

MGT521 Driving Cyber Change: Establishing a Culture of Protect, Detect, and Respond

MGT433 SANS Security Leadership: How to Build, Maintain & Measure a Mature Awareness Program GRC

SANS Security Leadership

POSTER



CISO Mind Map

Version 2.1

Vulnerability Management Maturity Model

For Cyber Leaders of Today and Tomorrow

sans.org/curricula/management

INT509_CISO_ML_v2.1_030

Based on CISO MindMap by Hafeez Rehman
@rfeez_rehman http://rfeezrehtman.com Used with permission.

Dominios de la Ciberseguridad (Usuario Final)

El universo de la ciberseguridad.



Juan Carlos Paris

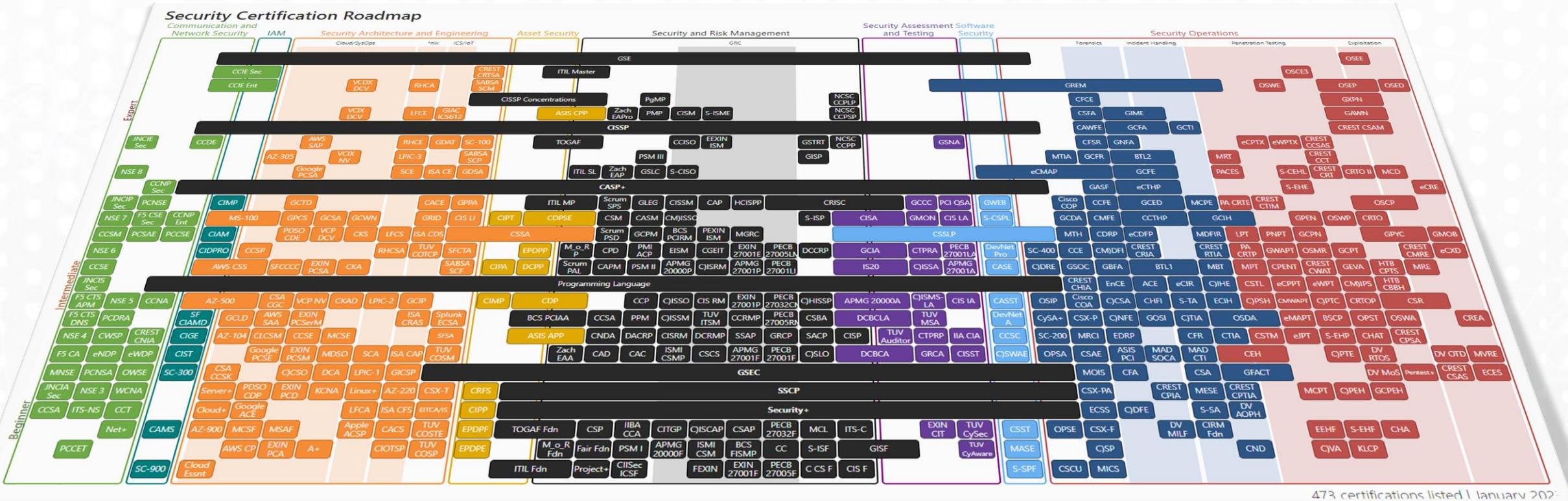
Cybersecurity Expert | Cloud | AI | TEDx | Oficial de Protección de Datos | Ingeniero Social | Especialista en Tecnología | Conferencista Nacional e Internacional | Ciberseguridad al alcance de todos...

[Ver perfil completo](#)

1. Seguridad de la red
2. Seguridad de la aplicación
3. Seguridad en la nube
4. Seguridad Móvil
5. Criptografía
6. Prevención de pérdida de datos (DLP)
7. Gestión de identidad y acceso (IAM)
8. Seguridad de terminales
9. Respuesta a incidentes
10. Inteligencia contra amenazas
11. Centro de operaciones de seguridad (SOC)
12. Gestión de eventos e información de seguridad (SIEM)
13. Pruebas de penetración
14. Gestión de vulnerabilidades
15. Capacitación en concientización sobre la seguridad
16. Análisis forense
17. Codificación segura
18. Seguridad web
19. Seguridad inalámbrica
20. Seguridad física
21. Gestión de riesgos
22. Gestión de Cumplimiento
23. Gobernanza, riesgo y cumplimiento (GRC)
24. Arquitectura de seguridad
25. Política y procedimientos de seguridad
26. Recuperación ante desastres
27. Planificación de la continuidad del negocio
28. Ciclo de vida de desarrollo seguro (SDL)
29. Sistemas de detección y prevención de intrusiones (IDPS)
30. Redes privadas virtuales (VPN)
31. Capa de conexión segura/Seguridad de la capa de transporte (SSL/TLS)
32. Autenticación multifactor (MFA)
33. Modelo de seguridad Zero Trust
34. Gestión de amenazas internas
35. Seguridad de la cadena de suministro
36. Seguridad de los sistemas de control industrial (ICS)
37. Seguridad del Internet de las Cosas (IoT)
38. Privacidad de datos
39. Análisis forense digital
40. Análisis de malware
41. Ingeniería Social
42. Caza de amenazas
43. Seguridad blockchain
44. Monitoreo de la Web Oscura
45. Capacitación y certificación en seguridad
46. Métricas e informes de seguridad
47. Gestión de contraseñas
48. Ejercicios del equipo rojo/equipo azul
49. Automatización de seguridad
50. Criptografía Cuántica
51. IA y Machine Learning
52. Destrezas Sociales e Interpersonales

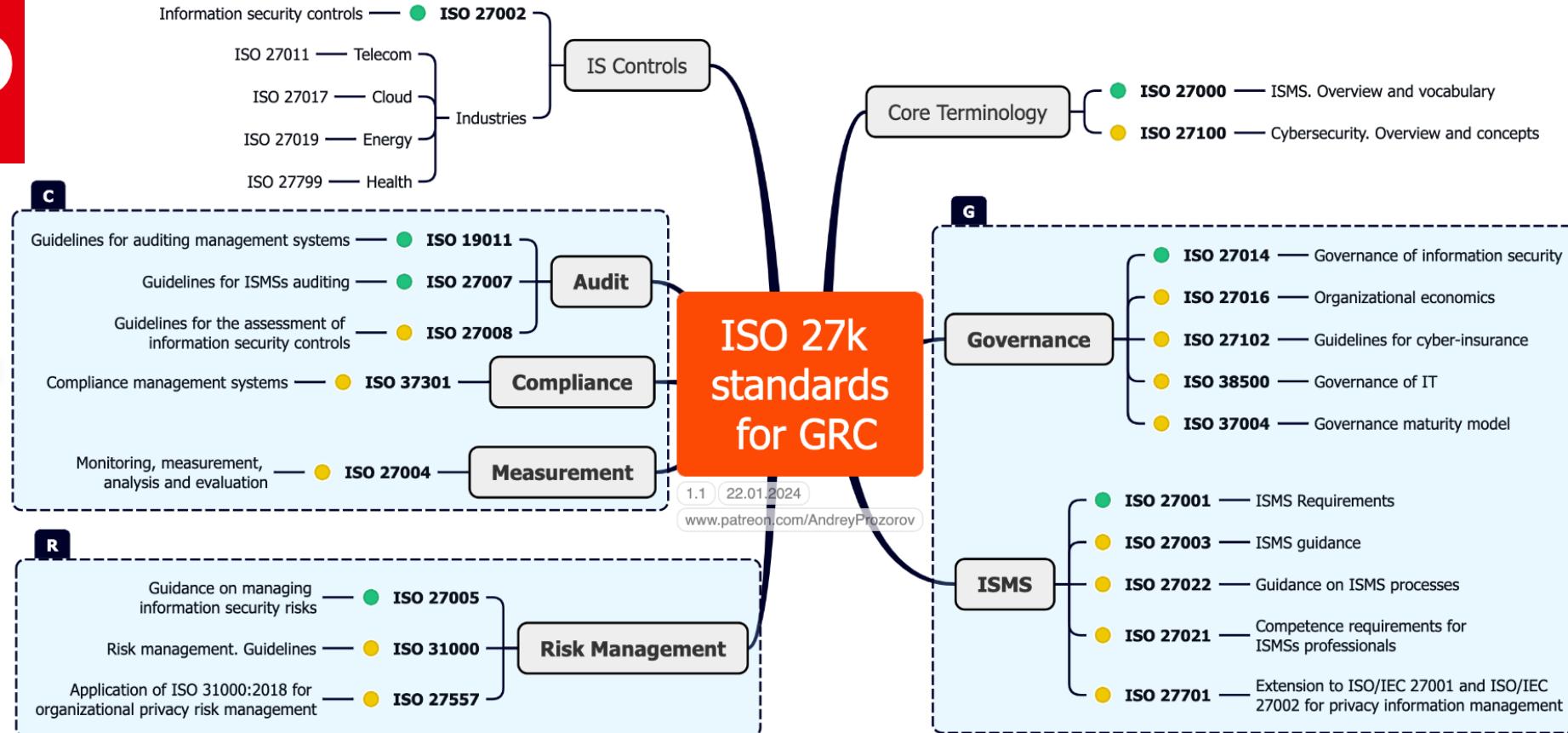
Certificaciones (Security Certification Roadmap)

Certificaciones profesionales en el mundo de la ciberseguridad.



Cumplimiento normativo de Ciberseguridad

(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)



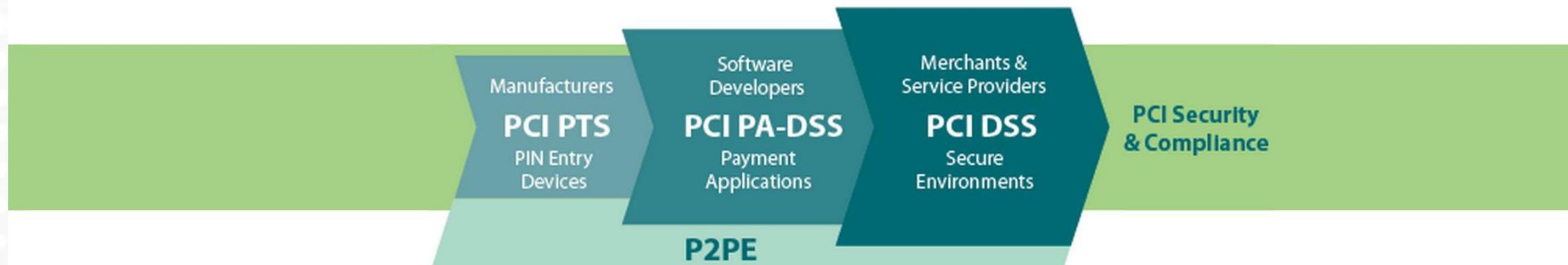
Cumplimiento normativo de Ciberseguridad

(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)



PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

Cumplimiento normativo de Ciberseguridad

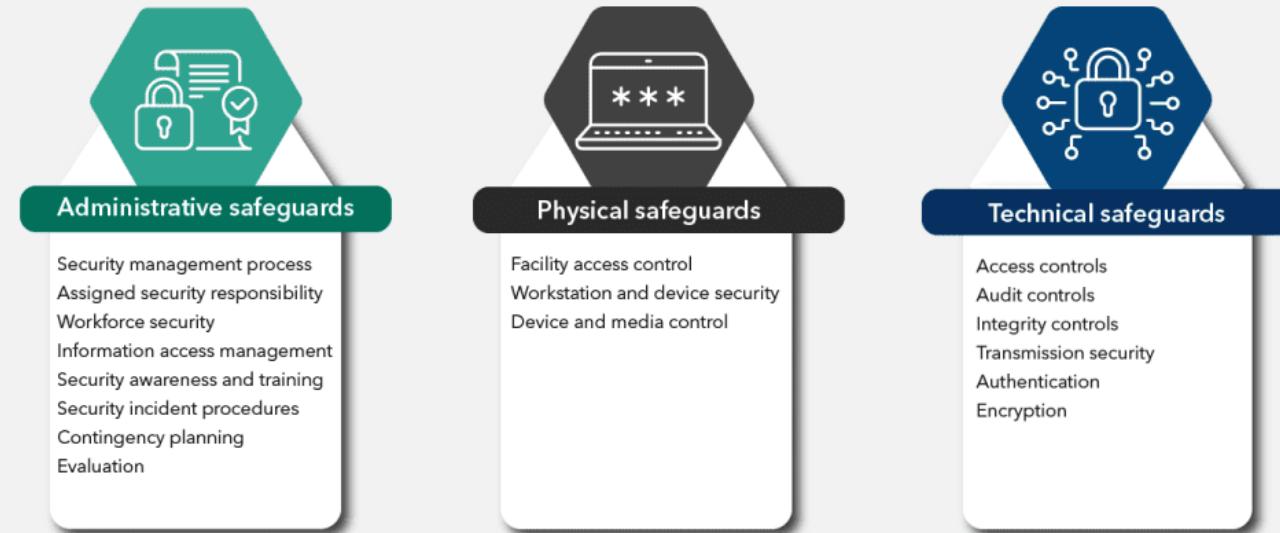
(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)



HIPAA, o la Ley de Portabilidad y Responsabilidad del Seguro de Salud (Health Insurance Portability and Accountability Act), es una legislación de Estados Unidos que establece estándares para la protección en el sector de la Salud.

Tanto los proveedores de atención médica como las organizaciones relacionadas con la atención médica, así como sus asociados comerciales que manejan información de salud, deben cumplir con las regulaciones de HIPAA.

3 key areas of HIPAA cybersecurity requirements



Alineación de HIPAA con NIST CSF

Cumplimiento normativo de Ciberseguridad

(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)

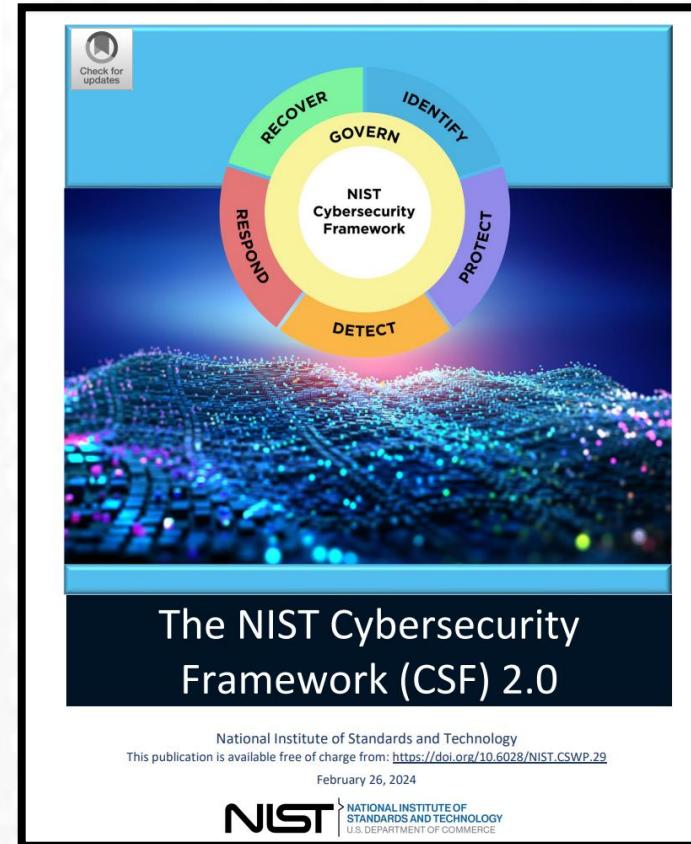


Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Cumplimiento normativo de Ciberseguridad

(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)



La Ley Sarbanes-Oxley (SOX) es una legislación federal en los Estados Unidos que establece estándares para la contabilidad de las empresas públicas y protege a los inversores al mejorar la precisión y confiabilidad de las revelaciones financieras corporativas. Las entidades que deben cumplir con SOX incluyen:

- Empresas públicas:** SOX se aplica principalmente a las empresas que cotizan en bolsa en los Estados Unidos. Esto incluye empresas que tienen valores registrados bajo la Comisión de Bolsa y Valores (SEC) de los Estados Unidos. Estas empresas están sujetas a diversas disposiciones de SOX, incluidas las secciones 302 y 404, que establecen requisitos específicos para la certificación de estados financieros y el control interno sobre la información financiera.
- Auditores externos:** SOX establece requisitos para la independencia y responsabilidad de los auditores externos que realizan auditorías de estados financieros para empresas públicas. Estos auditores deben cumplir con ciertas normas éticas y de calidad, así como proporcionar informes adicionales sobre los controles internos de la empresa.
- Miembros de la junta directiva y ejecutivos de la empresa:** Los directores ejecutivos (CEO) y los directores financieros (CFO) de empresas públicas tienen responsabilidades adicionales bajo SOX, incluida la certificación de la exactitud de los informes financieros y la implementación de controles internos efectivos sobre la información financiera.
- Entidades reguladoras:** Las entidades reguladoras, como la Comisión de Bolsa y Valores (SEC), tienen un papel clave en la aplicación de SOX y en la supervisión del cumplimiento de las empresas públicas con los requisitos de la ley.

En resumen, SOX está dirigido principalmente a empresas públicas y a aquellos que tienen responsabilidades significativas en relación con la precisión y la divulgación de la información financiera de estas empresas.

Cumplimiento GOV de Ciberseguridad

(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)



SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO IV
DEBERES Y RESPONSABILIDADES

CAPÍTULO V:
REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

CONTENIDO

- 1. ÁMBITO DE APLICACIÓN**
- 2. DEFINICIONES**
- 3. OBLIGACIONES GENERALES EN MATERIA DE CIBERSEGURIDAD**
- 4. ETAPAS**
 - 4.1. Prevención
 - 4.2. Protección y Detección
 - 4.3. Respuesta y Comunicación
 - 4.4. Recuperación y Aprendizaje

<https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1031729>

LEY N°. 1273 5 ENE 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".

EL CONGRESO DE COLOMBIA

DECRETA:

ARTÍCULO 1º. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO PRIMERO
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuerza de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269B: OBSTACULIZACIÓN ILEGAL DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTÍCULO 269C: INTERCEPCIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.



LEY ESTATUTARIA 1581 DE 2012
(Octubre 17)

Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011, Ver Decreto 255 de 2022.

Por la cual se dictan disposiciones generales para la protección de datos personales.

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1º. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2º. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

DECRETO 338 DE 2022
(8 DE MARZO)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN

COMUNICACIONES

"Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

En ejercicio de sus facultades constitucionales y legales, en especial las que le confiere el numeral 11 del artículo 189 de la Constitución Política y el artículo 43 de la Ley 489 de 1998,

CONSIDERANDO

Que, conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones -TIC-,(...), (...) las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones (...)"

Que, en virtud del numeral 2 del artículo 17 de la Ley 1341 de 2009, el Ministerio de Tecnologías de la Información y las Comunicaciones tiene entre sus objetivos "(...) 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación"

Cumplimiento GOV de Ciberseguridad

(ISO, PCI, HIPPA, SOX, NIST, SUPERFINANCIERA, GOV)

Documentos CONPES

En esta sección encuentra los documentos de políticas públicas (CONPES) que incluyen temas relacionados con la seguridad digital y que son liderados por la Dirección de Desarrollo Digital o Direcciones técnicas del Departamento Nacional de Planeación (DNP).

CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa

Este documento CONPES busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernetico (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

[Consulte el CONPES 3701](#)

[Vea el Plan de Acción y Seguimiento del CONPES3701](#)

CONPES 3854. Política Nacional de Seguridad Digital

Este documento CONPES busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

[Consulte el CONPES 3854](#)

[Consulte el CONPES 3854 Adenda](#)

[Vea el Plan de Acción y Seguimiento del CONPES3854](#)

CONPES 3995. Política Nacional de Confianza y Seguridad digital

Este documento CONPES busca establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

[Consulte el CONPES 3995](#)

[Vea el Plan de Acción y Seguimiento del CONPES3995](#)



Documento Conpes

Consejo Nacional de Política Económica y Social
República de Colombia
Departamento Nacional de Planeación

3701

LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA

Ministerio de Interior y de Justicia
Ministerio de Relaciones Exteriores
Ministerio de Defensa Nacional
Ministerio de Tecnologías de la Información y las Comunicaciones
Departamento Administrativo de Seguridad
Departamento Nacional de Planeación-DJSG-DIFP-DIES-OI
Fiscalía General

Versión aprobada

Bogotá D.C., 14 de julio de 2011



Proyecto del MinTIC para la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales pasa el primer debate

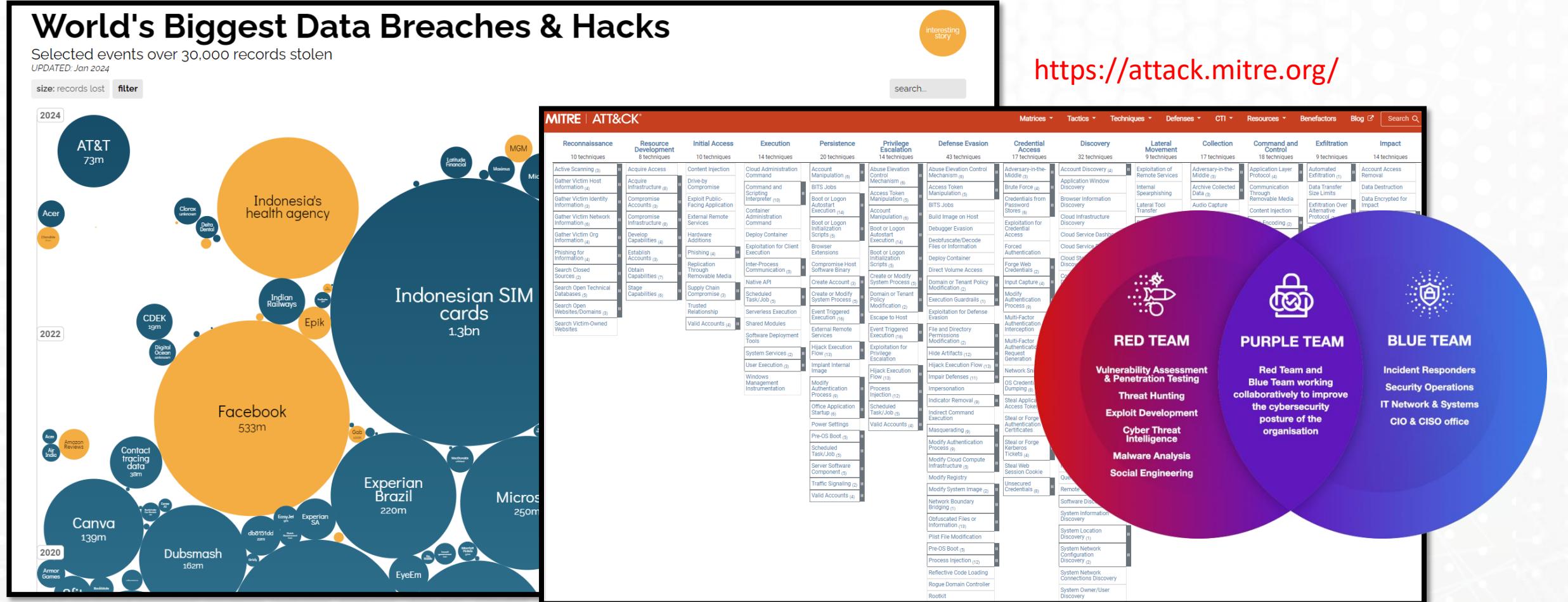
Nacional

Última actualización: Nov 01, 2023

https://www.dnp.gov.co/LaEntidad/_subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

La Ciberseguridad en el mundo corporativo

La Ciberseguridad en el mundo corporativo



La Ciberseguridad en el Hogar

La Ciberseguridad en el mundo corporativo

SEXTING: Les comarto un comercial de Movistar (2017) para alertar sobre los peligros de la suplantación de identidad y el "Sexting". Lo traigo a esta fecha por qué ahora los ataques son mucho más elaborados con DEEPFAKE.

Compartamos este video a nuestros familiares para crear conciencia.

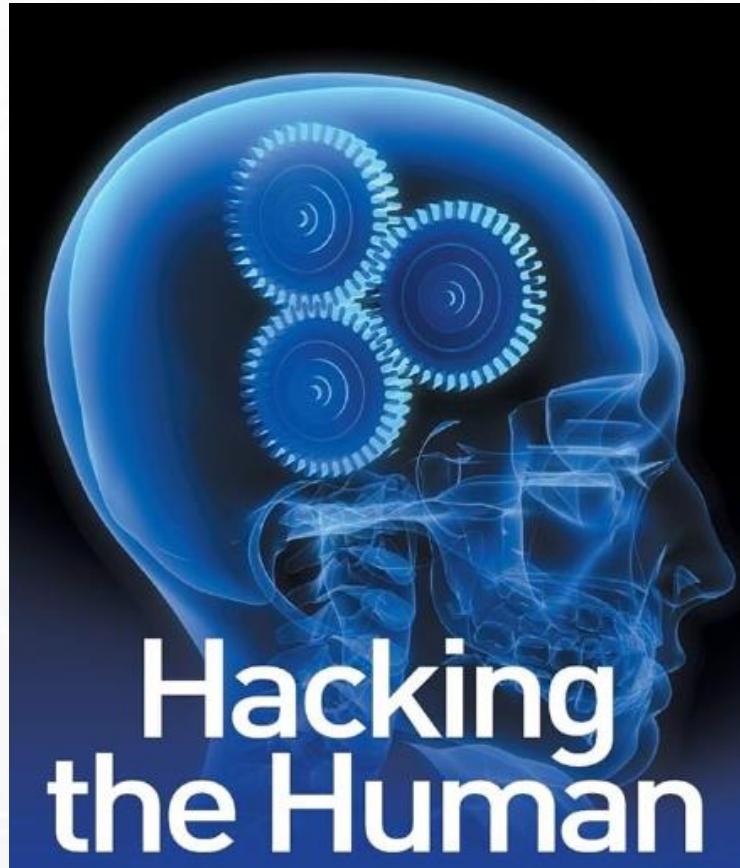
Video:

<https://www.youtube.com/watch?v=eZ00XG3cWKY>



Retos de la Ciberseguridad – Hacking Human

Retos de Ciberseguridad, Ataques actuales por medio de la AI, entre otros.



incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

INCIBE INCIBE-CERT CIUDADANÍA MENORES EMPRESAS EVENTOS ESPAÑA DIGITAL 2026

Tu Ayuda en Ciberseguridad Experiencia INCIBE Formación Programa Cibercooperantes Campañas Sala de prensa Información corporativa

Ingeniería social

“El engaño como arma del delito”

https://www.incibe.es/sites/default/files/docs/c14_pdf_infografia-tecnicas-ingenieria-social.pdf



Retos de la Ciberseguridad – Hacking con AI

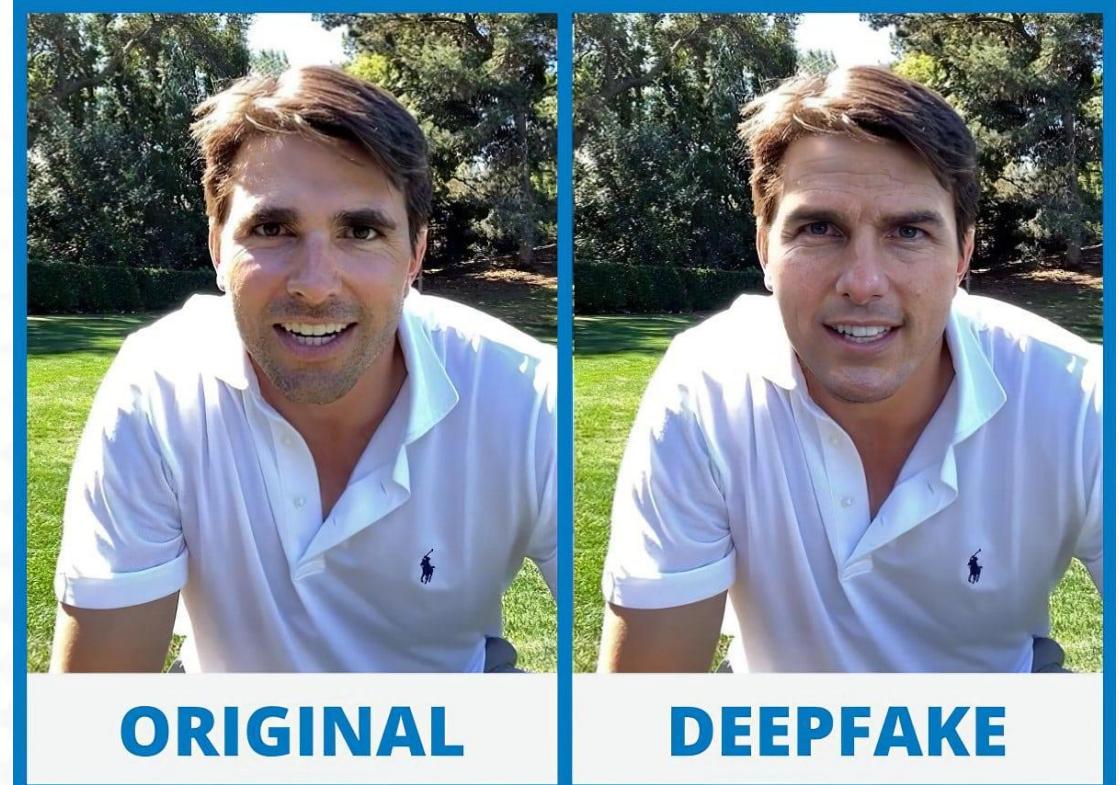
Retos de Ciberseguridad, Ataques actuales por medio de la AI, entre otros.



Un **DeepFake** es un video en el que se muestran imágenes falsas, habitualmente del rostro de una persona, que parecen ser reales y que se han producido utilizando inteligencia artificial.

<https://www.youtube.com/watch?v=JkUF40kPV4M>

[https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024#:~:text=Generative%20AI%20\(GenAI\)%2C%20unsecure,%2C%20according%20to%20Gartner%2C%20Inc.](https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024#:~:text=Generative%20AI%20(GenAI)%2C%20unsecure,%2C%20according%20to%20Gartner%2C%20Inc.)



Retos de la Ciberseguridad - RANSOMWARE

Retos de Ciberseguridad, Ataques actuales por medio de la AI, entre otros.



RANSOMEDVC

We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!

News: SONY.com data and access for sale

NOTICE: Downtime has been resolved, very sorry! PS: We need affiliates :))

Join Our Affiliate Program

SONY.COM / Post Date: 28.9.2023

Revenue: \$88,000,000,000 (\$88b)

- Sony Group Corporation, formerly Tokyo Telecommunications Engineering Corporation, and Sony Corporation, is a Japanese multinational conglomerate headquartered in Minato, Tokyo, Japan

We have successfully compromised all of sony systems. We wont ransom them! we will sell the data. due to sony not wanting to pay. DATA IS FOR SALE

R File tree: [link](#)

Sample Of Data: [link](#)

WE ARE SELLING IT

Contact us on tox asap!!!

Buy



385 Tipos de Ransomware a 2016

#	Extension	Extension Pattern	Ransom Note Filenames(s)	Comment	Encryption Algorithm	Also known as	Date Added/Modified	Decryptor	Info
1 LIST DOESN'T GET UPDATED ANYMORE									
NOTE: We initiated this list back in 2016 when adding a new ransomware occasionally was manageable as a side project. However, times have shifted, and ransomware has grown into a relentless pandemic. We're introducing AV vendors who are now responsible for maintaining this list. We're discontinuing this project. For historical reasons, this list was updated regularly from 2016 to 2018 and had sporadic updates in 2019.									
2									
3									
4	.enc	your_files_are_locked.htm	READ_ME.txt		AES(128)				
5	.777	_[timestamp]_Serial[8.777]	read_this_file.txt		XOR	Seleg			
6	.7z	e.g., _14-05-2016-11-59-40.7z	FILES_BACK.tot						
7	.7zR	7zR	READ_ME.TXT		AES	7zR-HONET			
8	.7zR	7zR	READ_IT.htm						
9	.Block	Block		Based on HiddenTea	AES(256)				
10	.Alfa	Alfa	...AreEncrypted	related to TeamRat					
11	.Alfa	Alfa	Alfa						
12	.Alpha	Alpha	ransom.html						
13	.Alpha	random	random(s)	READ HOW TO DECRYPT YOUR FILES.html					
14	.Alpha	encrypt		Unlock_files_randoms.html	AES(128)				
15	.Alpha			Read_Me (How Decrypt).htm	AES(128)	AlphaLocker			
16	.AMBA	AMBA							
17	.Angela	Angela		IPOTHET_MEHR.htm					
18	.Angela	Merkel		READ_ME.htm					
19	.Anger	Anger							
20	.Angry	Angry		READ_ME.txt		Demands 10 BTC			
21	.Anubis	Anubis							
22	.Apocalypse	Apocalypse		Decryption Instructions.htm	AES(256)				
23	.ApocalypseRM	ApocalypseRM		[filename].10*#characters#v0.1_How_To_Decrypt.txt		Fabianosware			
24	.ASNI	ASNI		decryptionservice@gmail.ru					
25	.Autolocky	Autolocky		*Contact_Here_To_Recover_Your_Files.htm					
26	.Awfulm88d7	Awfulm88d7		Where_my_Files.txt					
27				Read_Me_Txt					
28				How_To_Get_Back.tot					
29				HowToDecrypt.htm					
30				info.txt					
31				info.html					

<https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKhn5uTsdiJWdCEsGIM0Y0Hvmc5g/edit#gid=1325727307>

Retos de la Ciberseguridad – CLOUD Hacking

Retos de Ciberseguridad, Ataques actuales por medio de la AI, entre otros.

- Benchmark checks

- This will help you **understand the size** of the environment and **services used**
 - It will allow you also to find some **quick misconfigurations** as you can perform most of this tests with **automated tools**

- Services Enumeration

- You probably won't find much more misconfigurations here if you performed correctly the benchmark tests, but you might find some that weren't being looked for in the benchmark test.
 - This will allow you to know **what is exactly being used** in the cloud env
 - This will help a lot in the next steps

- Check exposed assets

- This can be done during the previous section, you need to **find out everything that is potentially exposed** to the Internet somehow and how can it be accessed.
 - Here I'm taking **manually exposed infrastructure** like instances with web pages or other ports being exposed, and also about other **cloud managed services that can be configured** to be exposed (such as DBs or buckets)
 - Then you should check **if that resource can be exposed or not** (confidential information? vulnerabilities? misconfigurations in the exposed service?)

- Check permissions

- Here you should **find out all the permissions of each role/user** inside the cloud and how are they used
 - Too **many highly privileged** (control everything) accounts? Generated keys not used?... Most of these check should have been done in the benchmark tests already
 - If the client is using OpenID or SAML or other **federation** you might need to ask them for further **information** about **how is being each role assigned** (it's not the same that the admin role is assigned to 1 user or to 100)
 - It's **not enough to find** which users has **admin** permissions `*:*`. There are a lot of **other permissions** that depending on the services used can be very **sensitive**.
 - Moreover, there are **potential privesc** ways to follow abusing permissions. All this things should be taken into account and **as much privesc paths as possible** should be reported.



- Check Integrations

- It's highly probable that **integrations with other clouds or SaaS** are being used inside the cloud env.
 - For **integrations of the cloud you are auditing** with other platform you should notify **who has access to (ab)use that integration** and you should ask **how sensitive** is the action being performed.
For example, who can write in an AWS bucket where GCP is getting data from (ask how sensitive is the action in GCP treating that data).
 - For **Integrations inside the cloud you are auditing** from external platforms, you should ask **who has access externally to (ab)use that integration** and check how is that data being used.
For example, if a service is using a Docker image hosted in GCR, you should ask who has access to modify that and which sensitive info and access will get that image when executed inside an AWS cloud.

¡GRACIAS!

¿Preguntas?



Asociación Colombiana
de Ingenieros

MITOS Y REALIDADES DE LA CIBERSEGURIDAD

(Lecciones aprendidas)

Mayo 16 de 2024



<https://www.linkedin.com/in/chacka0101/>



<https://github.com/chacka0101>

