Gobernanza en Ciberseguridad

Bogotá, Colombia

Oscar Colin

FREE WIFI

AGENDA

1. BIENVENIDA
2. ¿QUE ES LA GOBERNANZA?
3. MODELOS DE REFERENCIA
4. GOBERNANZA DE ESTADO, PAIS Y GOBIERNO.
5. BUENAS PRÁCTICAS.
6. TIPS & TRICKS.
7. CASOS PRÁCTICOS.

SIEMENS

Solo hay dos tipos de empresas: las que han sufrido un ataque y las que están a punto de sufrir un ataque.

CNN Colombia Gustavo Petro

Activan protocolo de emergencia en Colombia por ciberataque a proveedor de telecomunicaciones

CAMBIO

Iniciar sesión

lecciones Colombia 2026 | Foros | Tecnología | Deportes | Cultura | Empresas | Imaginar la D

TECNOLOGÍA · 11 Junio 2024 10:06 am

Colombia es el país más afectado por ataques cibernéticos en América Latina

ONES | BUSCAR

EL ECONOMISTA

ÚLTIMAS NOTICIAS | **TENDENCIAS:** TEMPORADA DE HURACANES | JORNADA LABORAL | ALIANZA EDUCATIVA | **MERCADOS:** ÍNDICES | DIVISAS

TECNOLOGÍA

Lectura

Hackers contra Colombia: las empresas sufren las consecuencias

¿QUE ES LA GOBERNANZA EN CIBERSEGURIDAD?
ROLES, OBJETIVOS Y RESPONSABILIDADES …

CONTROL

DIRECCIÓN

ENFOQUE

SIEMENS

GOBERNANZA (EJEMPLOS)

More Security-Related Functions and Business Stakeholders

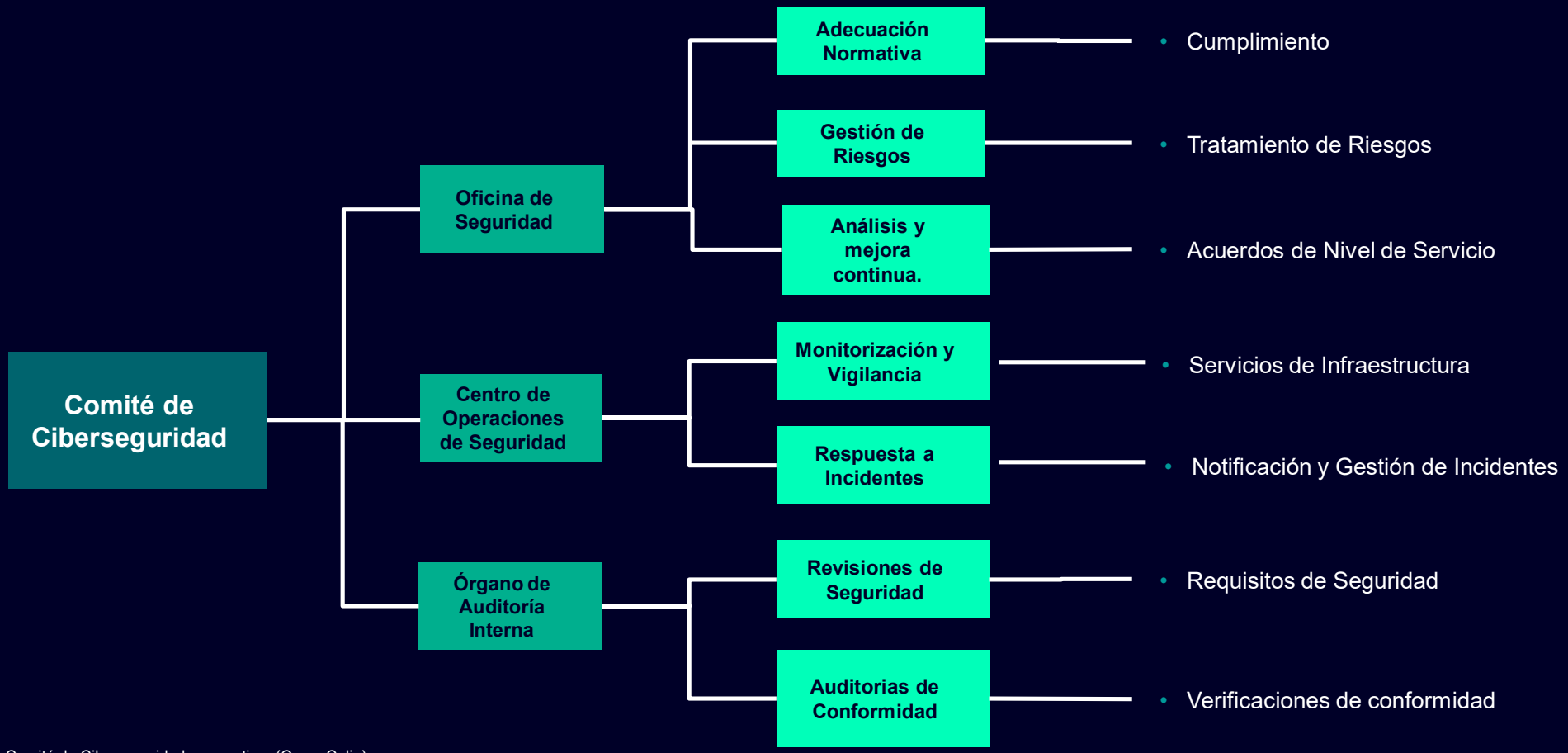
Dan Blum (2020). En *Rational Cybersecurity for Business* Springer. https://doi.org/10.1007/978-1-4842-5952-8_2

Competencias de la organización Cibersegura.

Tecnológico de Monterrey: Autor Anónimo

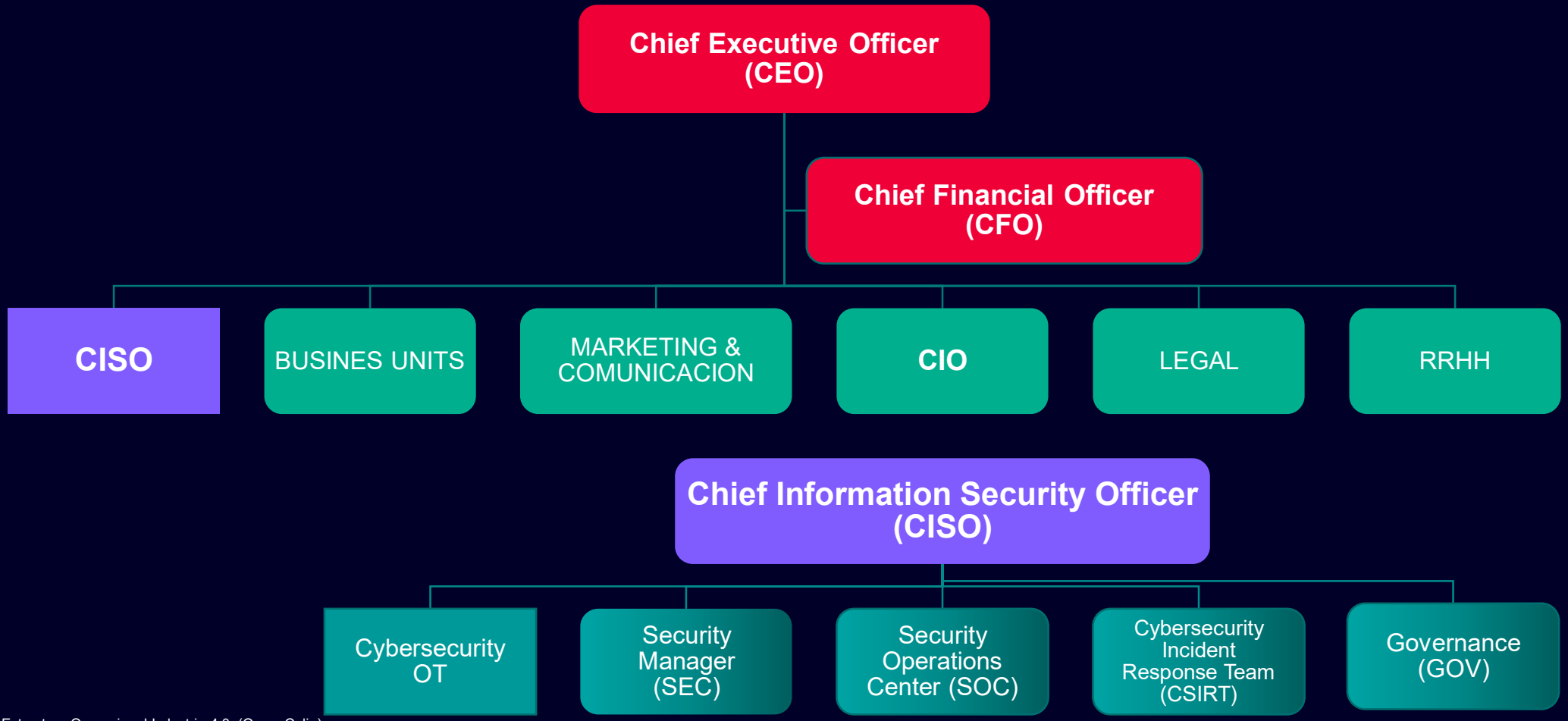
SIEMENS

GOBERNANZA (EJEMPLOS)



Comité de Ciberseguridad corporativa. (Oscar Colin)

ESTRUCTURA OPERACIONAL



Estructura Operacional Industria 4.0. (Oscar Colin)

MODELOS DE REFERENCIA
COBIT, NIST CSF2.0, ISO27001, CIS….

COBIT 2019

CIS Controls

ISO 27001

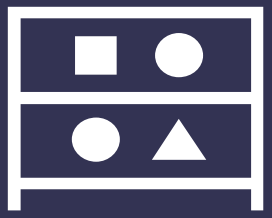
SIEMENS

GOBERNANZA A NIVEL ESTADO, PAÍS, GOBIERNO

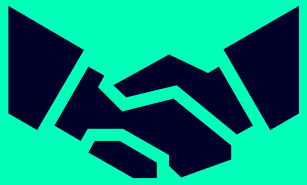
MARCO Y POLITICA DE CIBERSEGURIDAD

GESTIÓN DE LA CIBERSEGURIDAD

SEGURIDAD DE PRODUCTOS Y SOLUCIONES



CONCIENTIZACIÓN



MONITOREO DEL ESTADO

GESTION DE RIESGOS

CRA Cyber Resilience Act

NIS2

enisa

SIEMENS

BUENAS PRÁCTICAS
TELECOMUNICACIONES

SIEMENS

TIPS & TRICKS
EJECUCIÓN, PRIORIZACIÓN, CULTURA Y LIDERAZGO.

SIEMENS

DIAGRAMA RACI

RACI	
R (Responsible): Ejecuta la tarea.	**A (Accountable):** Aprueba la ejecución; responsable
C (Consulted): Aporta conocimiento; debe ser consultado.	**I (Informed):** Debe ser informado de la actividad.

Etapa	Actividad / Fase	País	Estado	Telecomunicaciones	Camaras e Industria
Preparación	Definición de protocolos	C	A	R	C
Preparación	Capacitación del personal	I	I	C	R
Preparación	Pruebas de seguridad (simulaciones)	C	R	C	C
Preparación	Inventario de recursos	I	C	I	R
Preparación	mplementación de controles preventivos (MFA, segment	I	C	R	R
Identificación	Gestión de inventario y usuarios autorizados	I	I	I	R
Identificación	Evaluación de riesgos y definición de niveles	C	A	C	C
Identificación	Clasificación de incidentes	R	A	C	C
Protección	Aplicación de MFA y segmentación	I	C	R	R
Protección	Monitoreo de accesos	R	I	I	I
Protección	Políticas de acceso y credenciales	I	C	I	R
Protección	Sensibilización de usuarios	I	R	I	I
Detección	Análisis de eventos (SIEM)	R	C	I	I
Detección	Generación de alertas	R	I	I	I
Detección	Verificación de registros y accesos anómalos	I	C	I	R
Detección	Correlación de IoCs	R	C	I	C
Detección	Análisis de comportamiento	R	C	I	C
Respuesta	Activación del CSIRT	R	A	I	I
Respuesta	Aislamiento de dispositivos / red	I	C	R	C
Respuesta	Análisis forense	I	R	C	C
Respuesta	Notificación a afectados	C	R	C	C
Respuesta	Implementación de contramedidas	I	R	R	C

RACI basado en NIST. (Oscar Colin)

SIEMENS

CASOS PRÁCTICOS
TELECOM

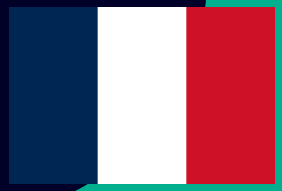
- Multa por brecha de datos.
- El CEO dirigió personalmente la nueva estrategia.

- 32 sitios de gobierno afectados.
- Acciones legales
- Servicios críticos impactados.

USD 880 M

Daño reputacional

- 600,000 registros expuestos.
- Vulnerabilidad por falta de hardening.



- Cortes de cableado.
- Vulnerabilidades físicas.

USD 20 M

1 día sin luz.

Reuters. (2025, julio 4). *South Korea orders SK Telecom to strengthen data security after leak*. Reuters. https://www.reuters.com/sustainability/boards-policy-regulation/south-korea-orders-sk-telecom-strengthen-data-security-after-leak-2025-07-04/

Bîzgă, A. (2020, julio 20). *Orange confirms ransomware attack compromising data of business solutions customers*. Bitdefender. https://www.bitdefender.com/en-us/blog/hotforsecurity/orange-confirms-ransomware-attack-compromising-data-of-business-solutions-customers

CONCLUSIONES

“Ignorar riesgos cibernéticos puede llevar al fracaso”

Natalia Oropeza. SIEMENS Global Chief Cybersecurity Officer & Chief Diversity Officer.

SIEMENS

CLICK IT !!!

SIEMENS

POTENCIEMOS COLOMBIA A TRAVÉS DE LA CIBERSEGURIDAD

Oscar Colin

Cybersecurity ST&EN
Americas Team Lead

oscar.colin@siemens.com