

# El rol del ciber-integrador para esta ciber-época

**Ramsés Gallego**

**CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt**

**Past International Vice President, ISACA, Board of Directors**

**Past President, ISACA Barcelona Chapter**

**Executive Vice President, Quantum World Association**

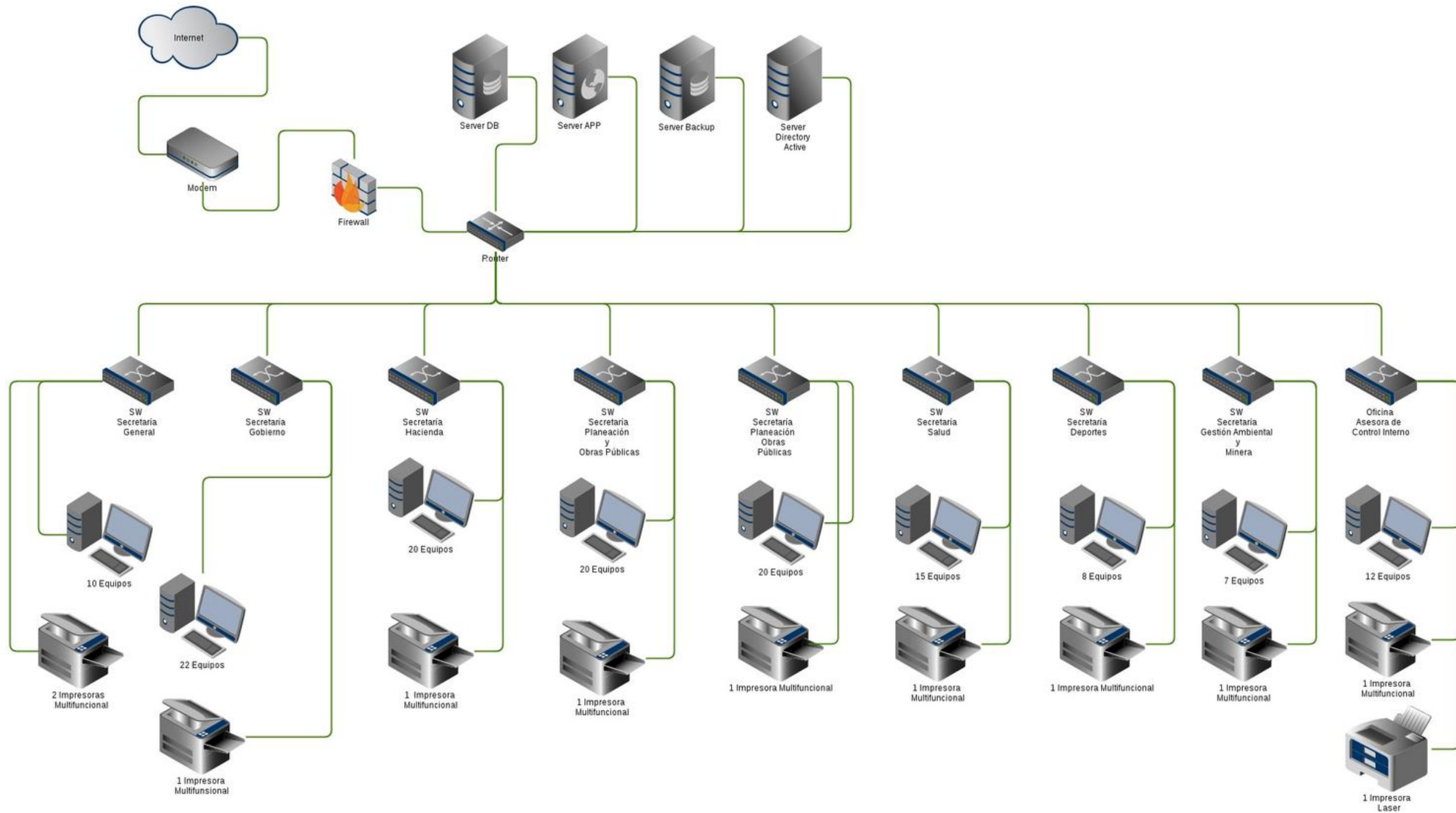
**Privacy by Design Ambassador, Government of Ontario, Canada**

**ramses.gallego@me.com**



**@ramsesgallego**





- Citrix (Netscaler) ( - 1)
- Extreme Networks ( - 3)
- Fortinet ( - 7)
- Hewlett-Packard ( - 5)
- HP (Colubris Networks) ( - 1)
- Juniper Networks ( - 11)
- Microsoft ( - 24)
- Palo Alto Networks ( - 5, - 2)
- Radware ( - 8)
- Ruckus Wireless ( - 5)

Sites ( - 235, - 5)

- All Sites ( - 235, - 5)
- Unassigned devices ( - 56)
- Alabama ( - 8)
- Alaska ( - 27, - 1)
- California ( - 44)
- Illinois ( - 18, - 1)
- New York ( - 1)
- Ohio ( - 49, - 1)
- Test ( )
- Texas ( - 32, - 2)
- BEAUMONT ( - 1)
- HAS-CO3-ST-R1.yourdomain.com (58.185.78.113)
- DALLAS ( - 24, - 1)
- HOUSTON ( - 7, - 1)

SQL Servers ( - 2)

Wireless Controllers ( - 9)

CDP Devices ( - 577)

IP Address Space

Open/close toolbar

«

»

📄

🔗

A

□

O

☁

A<sub>d</sub>-

A<sub>d</sub>+

A<sub>i</sub>-

A<sub>i</sub>+

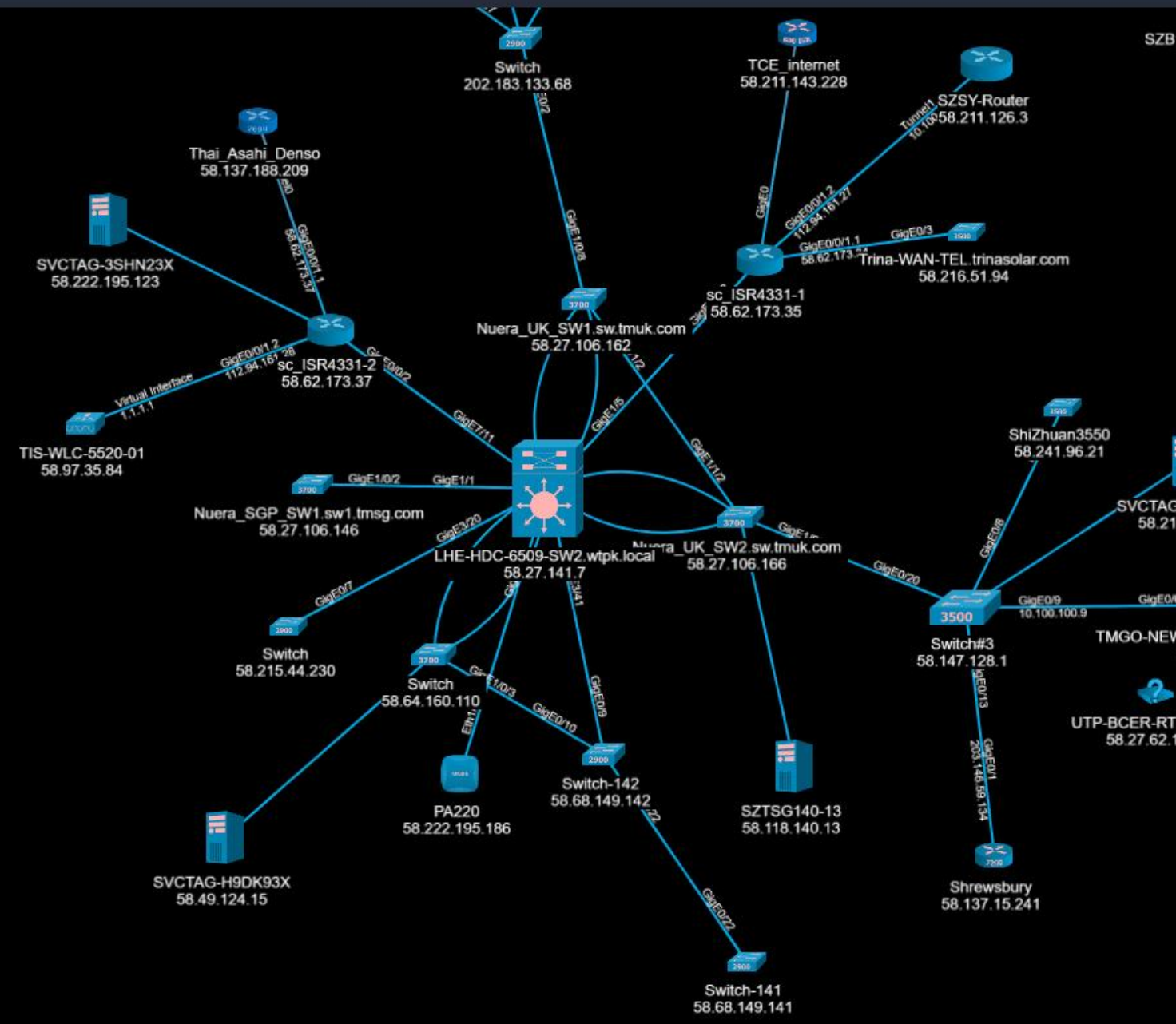
D-

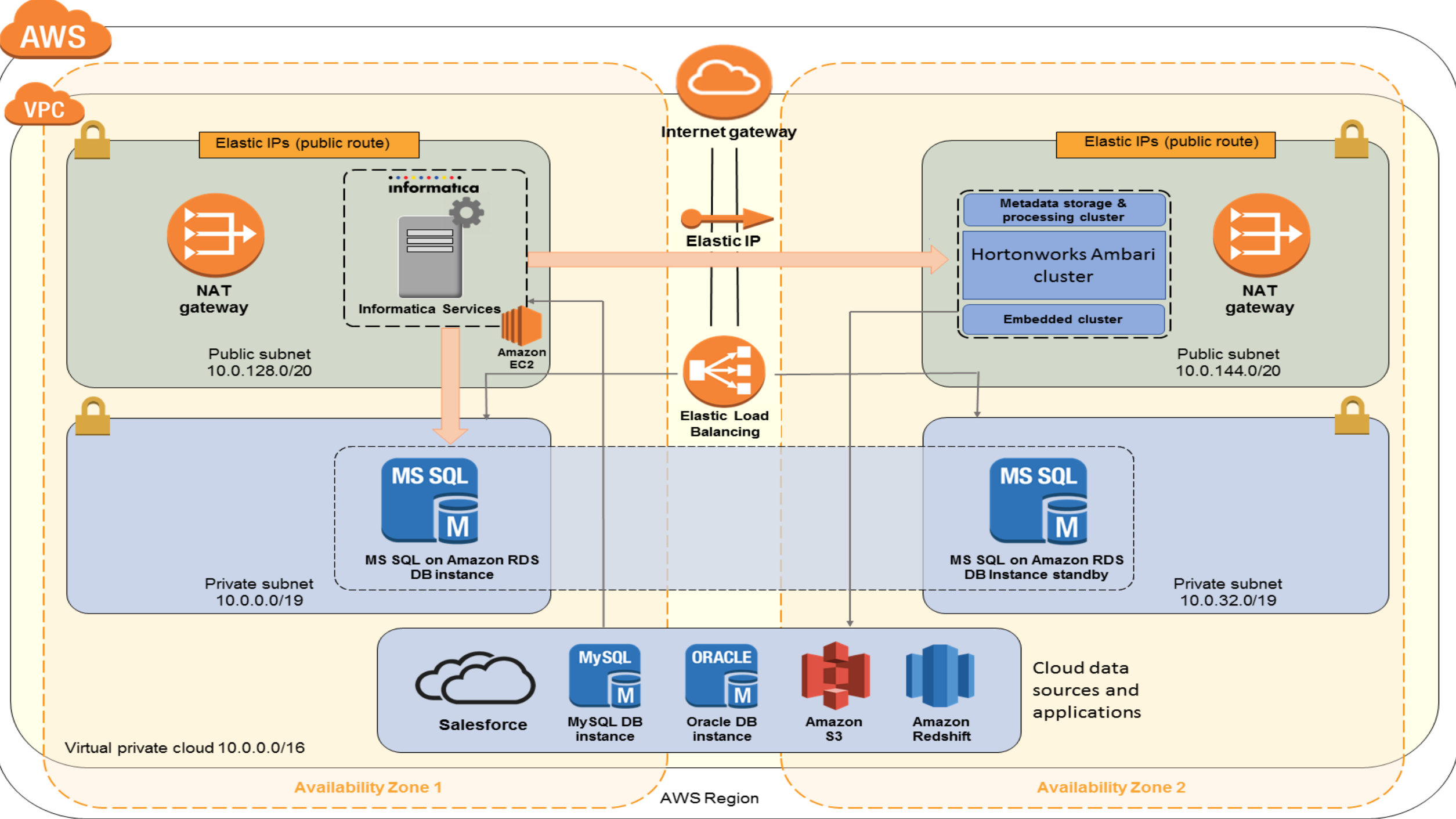
D+

🔍

🔍

4

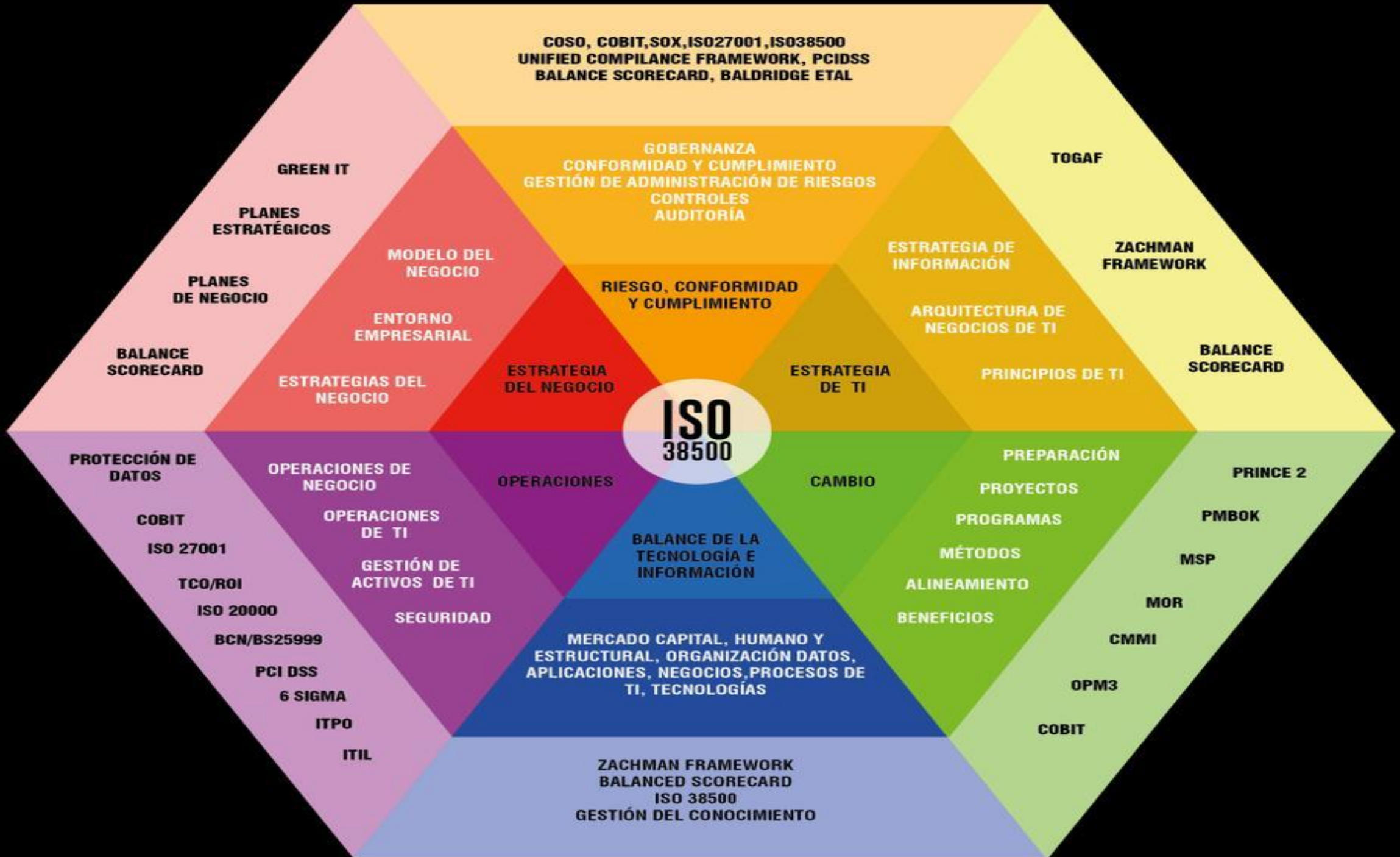




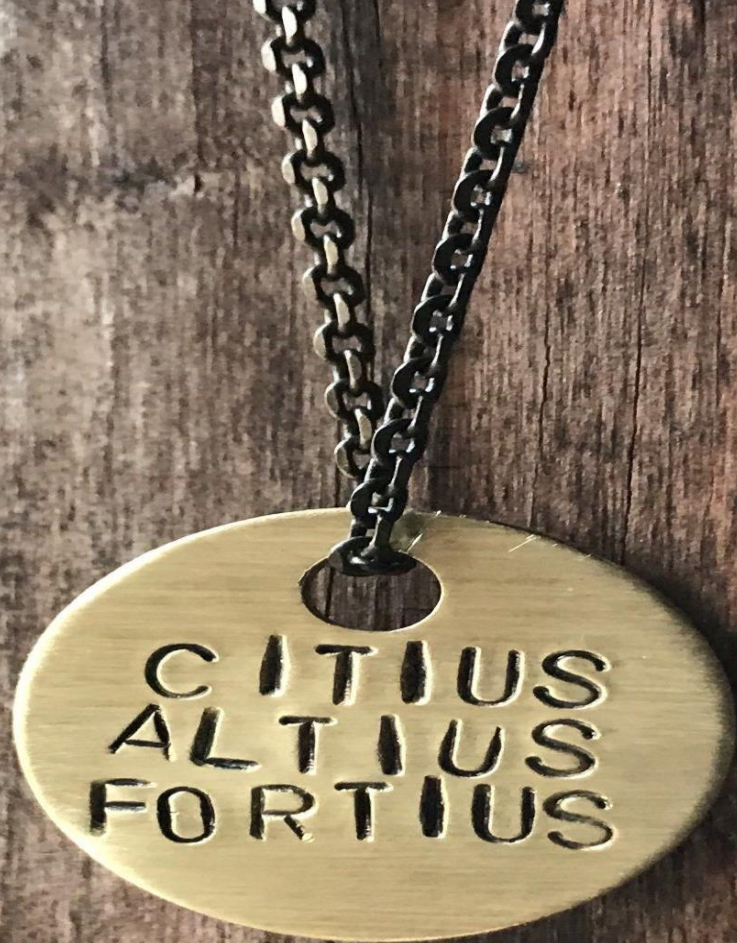












CITIUS  
ALTIUS  
FORTIUS



## CCN-STIC-800 Guías Esquema Nacional de Seguridad

La Sección CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad (RD 3/2010).

Las Guías sobre entornos tecnológicos que cumplen con el ENS figuran en la sección de Serie 500 (las actualizadas desde el mes de agosto de 2017 en adelante).

Buscar:  Mostrar 10  elementos

| Documento                                                                                                                                                                             | Publicado | Actualizado |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-------------------------------------------------------------------------------------|
| CCN-STIC 885A Guía de configuración segura para Office 365                                                                                                                            | Dic 2019  | Dic 2019    | <a href="#">PDF</a>                                                                 |
| CCN-STIC-884A Guía de configuración segura para Azure                                                                                                                                 | Dic 2019  | Dic 2019    | <a href="#">PDF</a>                                                                 |
| CCN-STIC-826 Implementación de Seguridad Nextcloud <ul style="list-style-type: none"><li>ENS (<a href="#">Anexo A</a> / <a href="#">Scripts</a>)</li></ul>                            | Nov 2019  | Nov 2019    | <a href="#">PDF</a>                                                                 |
| CCN-STIC-824 Información del Estado de Seguridad <ul style="list-style-type: none"><li><a href="#">Anexo C (SHA)</a></li></ul>                                                        | Nov 2012  | Oct 2019    | <a href="#">Descargar</a>                                                           |
| CCN-STIC-844 Manual de usuario de INES <ul style="list-style-type: none"><li><a href="#">Anexo</a></li><li><a href="#">Anexo II (SHA)</a></li><li><a href="#">Anexo III</a></li></ul> | Sep 2015  | Oct 2019    | <a href="#">Descargar</a>                                                           |
| CCN-STIC-882 Guía de Análisis de Riesgos para Entidades Locales                                                                                                                       | Jun 2019  | Jun 2019    | <a href="#">PDF</a><br><a href="#">Ejemplo</a>                                      |
| CCN-STIC-809 Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento                                                                                      | Jul 2010  | Jun 2019    | <a href="#">Descargar</a>                                                           |
| CCN-STIC-883 Guía de implantación del ENS para Entidades Locales                                                                                                                      | May 2019  | May 2019    | <a href="#">Descargar</a>                                                           |
| CCN-STIC-801 Responsabilidades y Funciones en el ENS                                                                                                                                  | Abr 2010  | Abr 2019    | <a href="#">Descargar</a>                                                           |
| CCN-STIC-819 Medidas Compensatorias                                                                                                                                                   | Oct 2018  | Oct 2018    | <a href="#">Descargar</a>                                                           |

Mostrando de 1 a 10 de 60 elementos

Anterior [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [Siguiente](#)

## 100 Procedimientos

La Serie CCN-STIC-100 establece el marco común de actuación en los procesos de acreditación, certificación TEMPEST, gestión de material de cifra y de cualquier otro campo que se considere.

Buscar:  Mostrar 10  elementos

| Documento                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Publicado | Actualizado |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-------------------------------------------------------------------------------------|
| CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Dic 2017  | Nov 2019    | <a href="#">Descargar</a>                                                           |
| CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC <ul style="list-style-type: none"><li>Anexo A.1: Control de Acceso a Red (NAC)</li><li>Anexo A.2: Dispositivos Biométricos</li><li>Anexo A.3: Dispositivos Single Sign-On</li><li>Anexo A.4: Servidores de Autenticación</li><li>Anexo A.6: Gestión de Acceso Privilegiado (PAM)</li><li>Anexo B.1: Anti-virus/EPP (ENDPOINT PROTECTION PLATFORM)</li><li>Anexo B.1M: Anti-virus/EPP (ENDPOINT PROTECTION PLATFORM)</li><li>Anexo B.2: EDR (ENDPOINT DETECTION AND RESPONSE)</li><li>Anexo B.3: Herramientas de gestión de red</li><li>Anexo B.4: Herramientas de actualización de sistemas</li><li>Anexo B.5: Herramientas de filtrado de navegación</li><li>Anexo B.6: Sistemas de gestión de eventos de seguridad (SIEM)</li><li>Anexo B.6.M: Sistemas de gestión de eventos de seguridad</li><li>Anexo B.8: Herramientas de gestión de dispositivos móviles (MDM)</li><li>Anexo C.1: Dispositivos de prevención y detección de intrusiones</li><li>Anexo C.2: Sistemas Honeypot/Honeynet</li><li>Anexo C.3: Captura, Monitorización y Análisis de Tráfico</li><li>Anexo D.1: Enrutadores</li><li>Anexo D.1M: Enrutadores</li><li>Anexo D.2: Switches</li><li>Anexo D.2.M: Switches</li><li>Anexo D.3: Cortafuegos</li><li>Anexo D.4: Proxies</li><li>Anexo D.5: Dispositivos de Red Inalámbricos</li><li>Anexo D.6: Pasarelas seguras de intercambio de datos</li><li>Anexo D.7: Diodo de datos</li><li>Anexo D.8.A: Redes privadas virtuales: IPSEC</li><li>Anexo D.8.B: Redes privadas virtuales: SSL</li><li>Anexo D.9: Herramientas para comunicaciones móviles seguras</li><li>Anexo E.1: Almacenamiento cifrado de datos</li><li>Anexo E.2: Cifrado offline</li><li>Anexo E.3: Herramientas de Borrado Seguro</li><li>Anexo E.4: Sistemas de prevención de fugas de datos</li><li>Anexo E.5: Herramientas para firma Electrónica</li><li>Anexo F.1: Dispositivos móviles</li></ul> | Nov 2017  | Sep 2019    | <a href="#">Descargar</a>                                                           |





## ATTACK ORIGINS

| #   | Country       |
|-----|---------------|
| 801 | China         |
| 358 | United States |
| 34  | Hong Kong     |
| 28  | Netherlands   |
| 28  | Taiwan        |
| 27  | Brazil        |
| 22  | Mil/Gov       |
| 22  | Portugal      |
| 17  | Canada        |
| 17  | Russia        |

## ATTACK TARGETS

| #    | Country       |
|------|---------------|
| 1280 | United States |
| 67   | Hong Kong     |
| 21   | Spain         |
| 20   | Canada        |
| 18   | Portugal      |
| 17   | Mil/Gov       |
| 8    | Netherlands   |
| 8    | Romania       |
| 8    | Italy         |
| 7    | Australia     |

## ATTACKS

| Timestamp              | Attacker                   |                          |                 | Target                       |            | Type  |
|------------------------|----------------------------|--------------------------|-----------------|------------------------------|------------|-------|
|                        | Organization               | Location                 | IP              | Location                     | Service    | Port  |
| 2014-07-08 11:14:07.37 | TMN Wifi Customers         | unknown, Portugal        | 88.214.180.212  | Saint Louis, United States   | isakmp     | 500   |
| 2014-07-08 11:14:07.75 | CHINANET-HN Hengyang       | Changsha, China          | 218.77.79.43    | Scotts Valley, United States | http-alt   | 8080  |
| 2014-07-08 11:14:08.22 | PTCL                       | Islamabad, Pakistan      | 182.186.176.116 | Kirksville, United States    | telnet     | 23    |
| 2014-07-08 11:14:08.32 | CariNet                    | San Diego, United States | 71.6.135.131    | Kirksville, United States    | pop3s      | 995   |
| 2014-07-08 11:14:09.26 | Webhosting.Net             | Miami, United States     | 67.215.180.74   | Miami, United States         | CrazyNet   | 17500 |
| 2014-07-08 11:14:10.17 | CariNet                    | San Diego, United States | 66.240.192.138  | Kirksville, United States    | dict       | 2628  |
| 2014-07-08 11:14:10.65 | Webhosting.Net             | Miami, United States     | 67.215.180.69   | Miami, United States         | netbios-ns | 137   |
| 2014-07-08 11:14:11.06 | Blind Ferret Entertainment | Montreal, Canada         | 174.142.19.173  | Montreal, Canada             | CrazyNet   | 17500 |

## ATTACK TYPES

| #   | Service          | Port  |
|-----|------------------|-------|
| 492 | ssh              | 22    |
| 228 | ms-term-services | 3389  |
| 187 | http             | 80    |
| 46  | CrazyNet         | 17500 |
| 38  | http-alt         | 8080  |
| 35  | snmp             | 161   |
| 29  | netbios-dgm      | 138   |
| 27  | swx              | 7331  |

[in](#)
[Twitter](#)
[f](#)
[YouTube](#)
[g+](#)







HOMO HOMINI LUPUS EST.

真 Night



# Implementing the NIST Cybersecurity Framework

| Function Unique Identifier | Function | Category Unique Identifier | Category                                         |
|----------------------------|----------|----------------------------|--------------------------------------------------|
| ID                         | Identify | AM                         | Asset Management                                 |
|                            |          | BE                         | Business Environment                             |
|                            |          | GV                         | Governance                                       |
|                            |          | RA                         | Risk Assessment                                  |
|                            |          | RM                         | Risk Management                                  |
| PR                         | Protect  | AC                         | Access Control                                   |
|                            |          | AT                         | Awareness and Training                           |
|                            |          | DS                         | Data Security                                    |
|                            |          | IP                         | Information Protection Processes and Information |
|                            |          | PT                         | Protective Technology                            |
| DE                         | Detect   | AE                         | Anomalies and Events                             |
|                            |          | CM                         | Security Continuous Monitoring                   |
|                            |          | DP                         | Detection Processes                              |
| RS                         | Respond  | CO                         | Communications                                   |
|                            |          | AN                         | Analysis                                         |
|                            |          | MI                         | Mitigation                                       |
|                            |          | IM                         | Improvements                                     |
| RC                         | Recover  | RP                         | Recovery Planning                                |
|                            |          | IM                         | Improvements                                     |
|                            |          | CO                         | Communications                                   |











- ✓ LEADERSHIP
- ✓ TEAMWORK
- ✓ COMMUNICATION

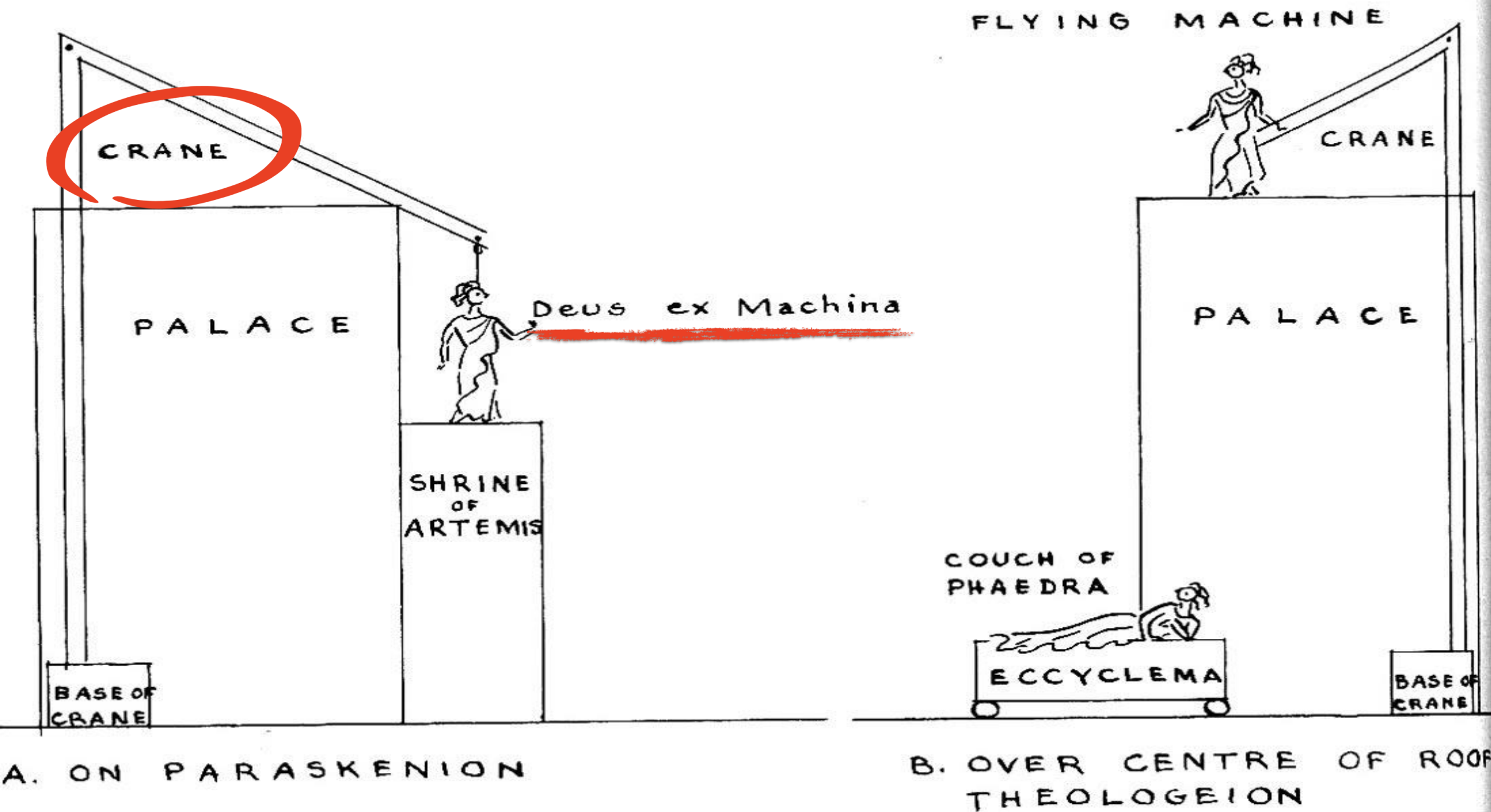


# INNOVATION









```
15 hSnapshot = CreateToolhelp32Snapshot(2u, 0);
16 if ( hSnapshot != -1 )
17 {
18     pe.dwSize = 556;
19     if ( Process32FirstW(hSnapshot, &pe) )
20     {
21         do
22         {
23             init_key = 0x12345678;
24             u0 = 0;
25             exe_name_len = wcslen(pe.szExeFile);
26             do
27             {
28                 u2 = 0;
29                 if ( exe_name_len )
30                 {
31                     iter_1 = u0;
32                     do
33                     {
34                         u4 = &init_key + (iter_1 & 3);
35                         u5 = (u4 ^ LOBYTE(pe.szExeFile[u2++])) - 1; // index bytes of the key
36                                                                    // by (iterator mod 4)
37                         ++iter_1;
38                         u4 = u5;
39                     }
40                     while ( u2 < exe_name_len );
41                 }
42                 ++u0;
43             }
44             while ( u0 < 3 );
45             if ( init_key == 0x2E214B44 ) // "AUP.exe" (Kaspersky AU)
46             {
47                 process_flag &= 0xFFFFFFFF7;
48             }
49             else if ( init_key == 0x6403527E || init_key == 0x651B3005 ) //
50                                                                    // 0x6403527E - "ccSvcHst.exe" (Symantec)
51                                                                    // 0x651B3005 - "NS.exe" (Norton Security)
52             {
53                 process_flag &= 0xFFFFFFFFB;
54             }
55         }
56         while ( Process32NextW(hSnapshot, &pe) );
57     }
58     CloseHandle(hSnapshot);
59 }
60 return process_flag;
61 }
```

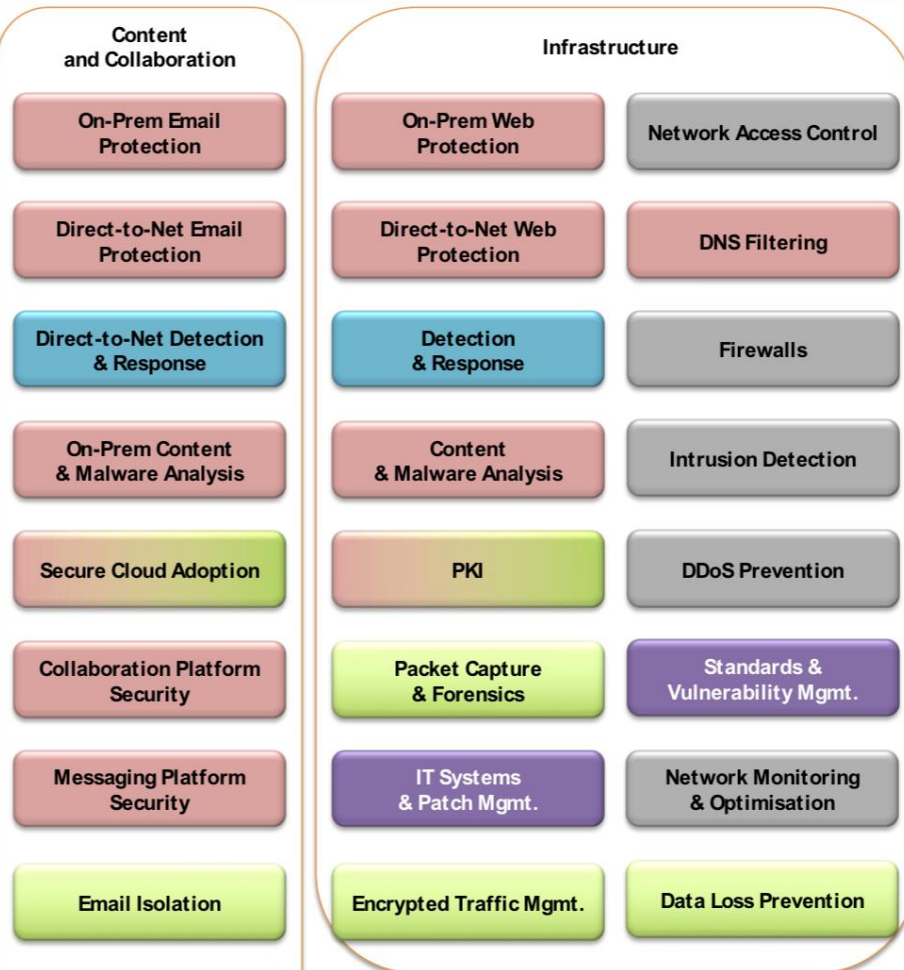
```
else if ( init_key == 0x6403527E || init_key == 0x651B3005 )//
```

```
// 0x6403527E - "ccSvcHst.exe" (Symantec)
```

```
// 0x651B3005 - "NS.exe" (Norton Security)
```



# Best Practice Security Architecture Framework



## Governance, Risk and Compliance

Risk Dashboard

3rd Party Risk Mgmt.

Regulatory Compliance

Risk Statistics

## Identity and Access Management

Single Sign-On

Multi-Factor Authentication

Privileged Access Management

Identity Management

## Internet of Things

Behavioural Security Engine

USB Sanitisation

## Security Operations Centre

Security Monitoring

Security Log Collection

Threat Investigation & Response

Malware Analysis

Event Ticketing

Packet Capture & Forensics

Workflow Automation

Integration Platform

Threat Intelligence Feed

## Technical Services

Premium Support

Value Realisation

## End-User Devices

Endpoint Protection

Active Directory Defence

Detection & Response

APT & Sandboxing

System Hardening

Deception

Endpoint Device & Patch Mgmt.

Browser Isolation

Endpoint Encryption

Data Loss Prevention

Mobile Threat Protection

Compliance Mgmt.

## Compute, Storage & Applications

Cloud Security Posture

Workload Protection

Cloud Storage Security

WAF & Reverse Proxy

Secure Cloud Adoption

Server Malware Protection

Static & Dynamic Code Analysis

System Hardening

Malware for Storage

DLP for Storage

DLP for Cloud

Cloud App Anti-Malware

## Data

Data Encryption

Data Loss Prevention

Data Classification

User Entity Behaviour Analytics

## Services

Incident Response

Actor Intelligence

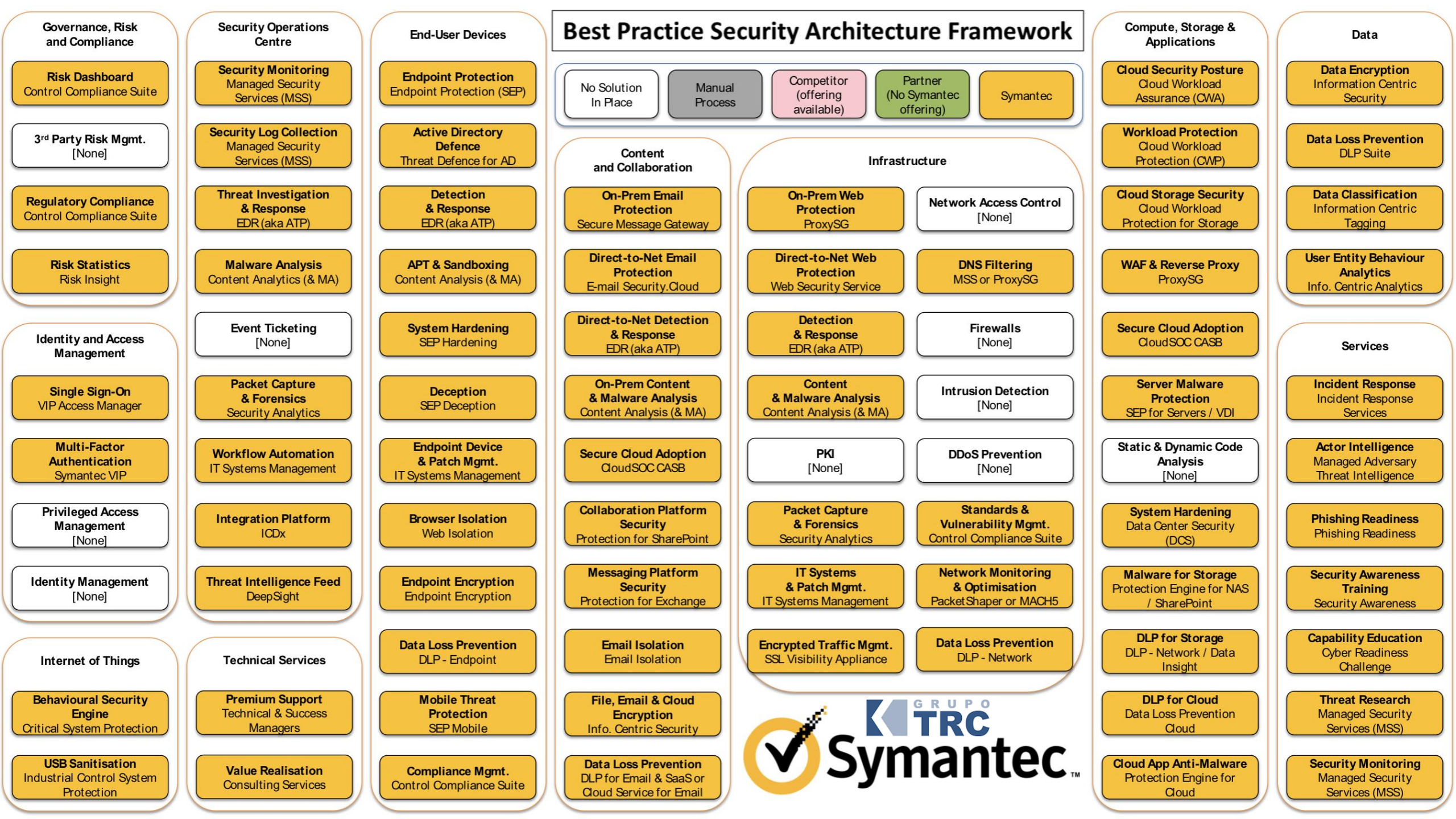
Phishing Readiness

Security Awareness Training

Capability Education

Threat Research

Security Monitoring



Experiment

Method



# GRACIAS

## El rol del ciber-integrador para esta ciber-época

**Ramsés Gallego**

**CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt**

**Past International Vice President, ISACA, Board of Directors**

**Past President, ISACA Barcelona Chapter**

**Executive Vice President, Quantum World Association**

**Privacy by Design Ambassador, Government of Ontario, Canada**

**ramses.gallego@me.com**



**@ramsesgallego**

