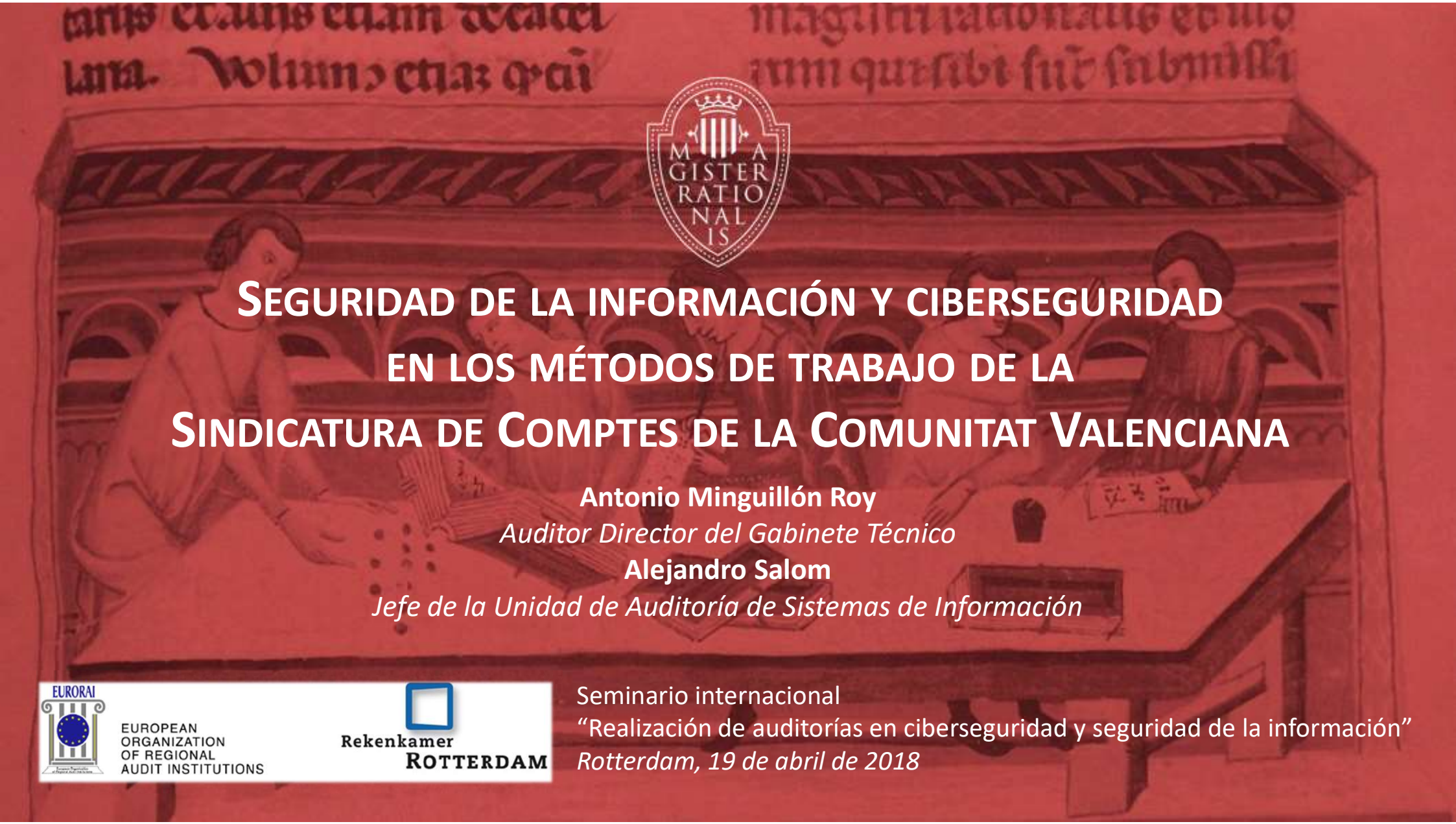


SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN LOS MÉTODOS DE TRABAJO DE LA SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Antonio Minguillón Roy

Auditor Director del Gabinete Técnico

Alejandro Salom

Jefe de la Unidad de Auditoría de Sistemas de Información

EUROPEAN ORGANIZATION OF REGIONAL AUDIT INSTITUTIONS

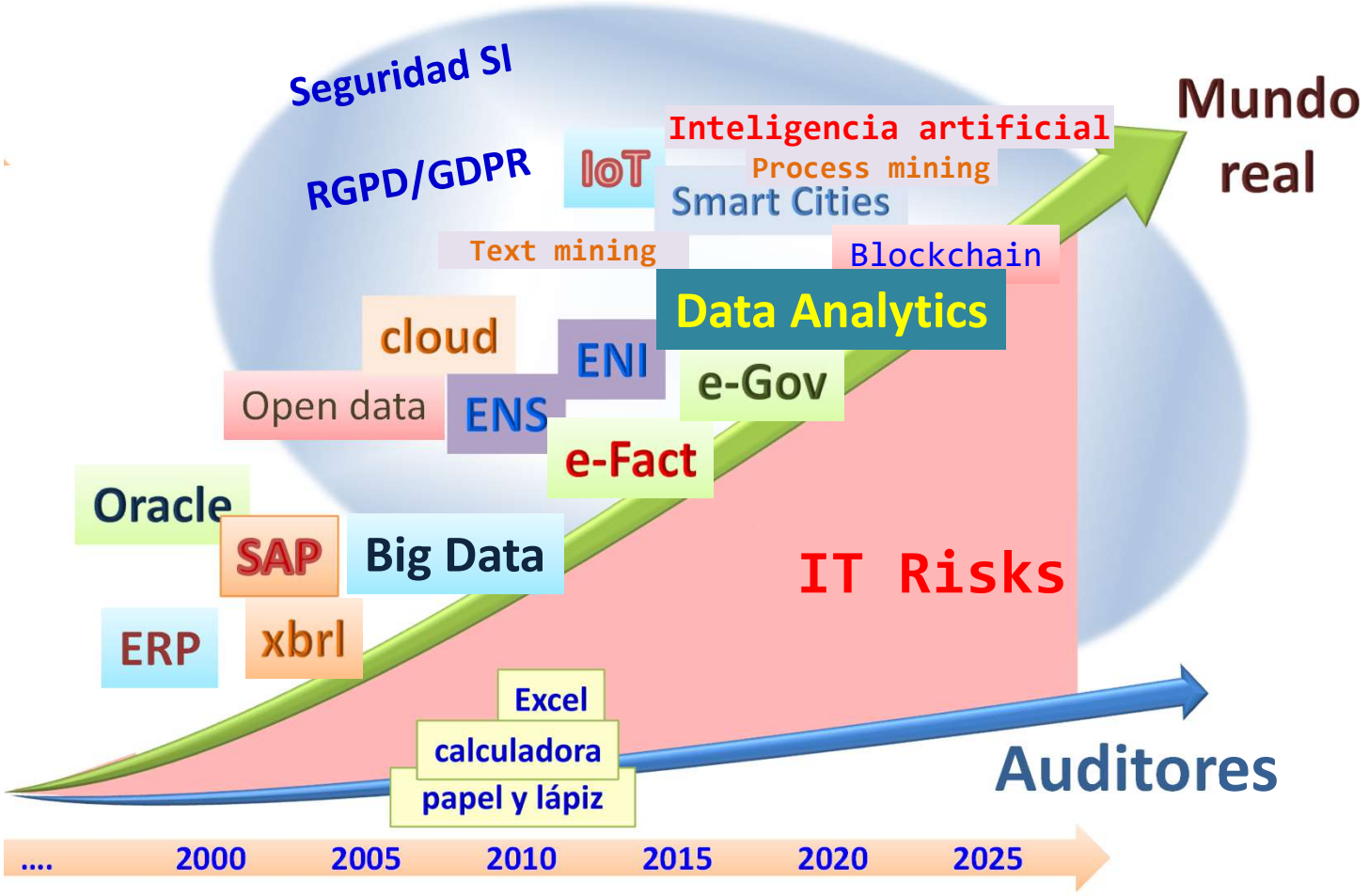
Rekenkamer ROTTERDAM

Seminario internacional

"Realización de auditorías en ciberseguridad y seguridad de la información"

Rotterdam, 19 de abril de 2018

La brecha digital



"… en su mayor parte, ***los auditores utilizan procesos anticuados que no son muy diferentes de los utilizados hace 50 años****, excepto por que han sido computerizados.*

El énfasis se ha puesto en mejorar la eficiencia, y aunque la eficacia ha mejorado también, no se ha dado el salto cualitativo que la tecnología permite".

AICPA,
White Paper
Agosto 2014

Principales retos que deben enfrentar las RAI

- Administración electrónica
- Big Data
- Ciberseguridad
- Análisis digital
- Visualización de datos
- Tecnologías cognitivas (IA)

Digital Transformation ***(¿Revolution?)***

- *Lucha contra el fraude y la corrupción*
- *Informes más útiles y comprensibles*
- *Calidad de las auditorías*
- *Implantar las nuevas normas técnicas*
- *Auditorías operativas y medioambientales*

RIESGOS

OPORTUNIDADES

ACCIÓN

Importancia de los ciber incidentes

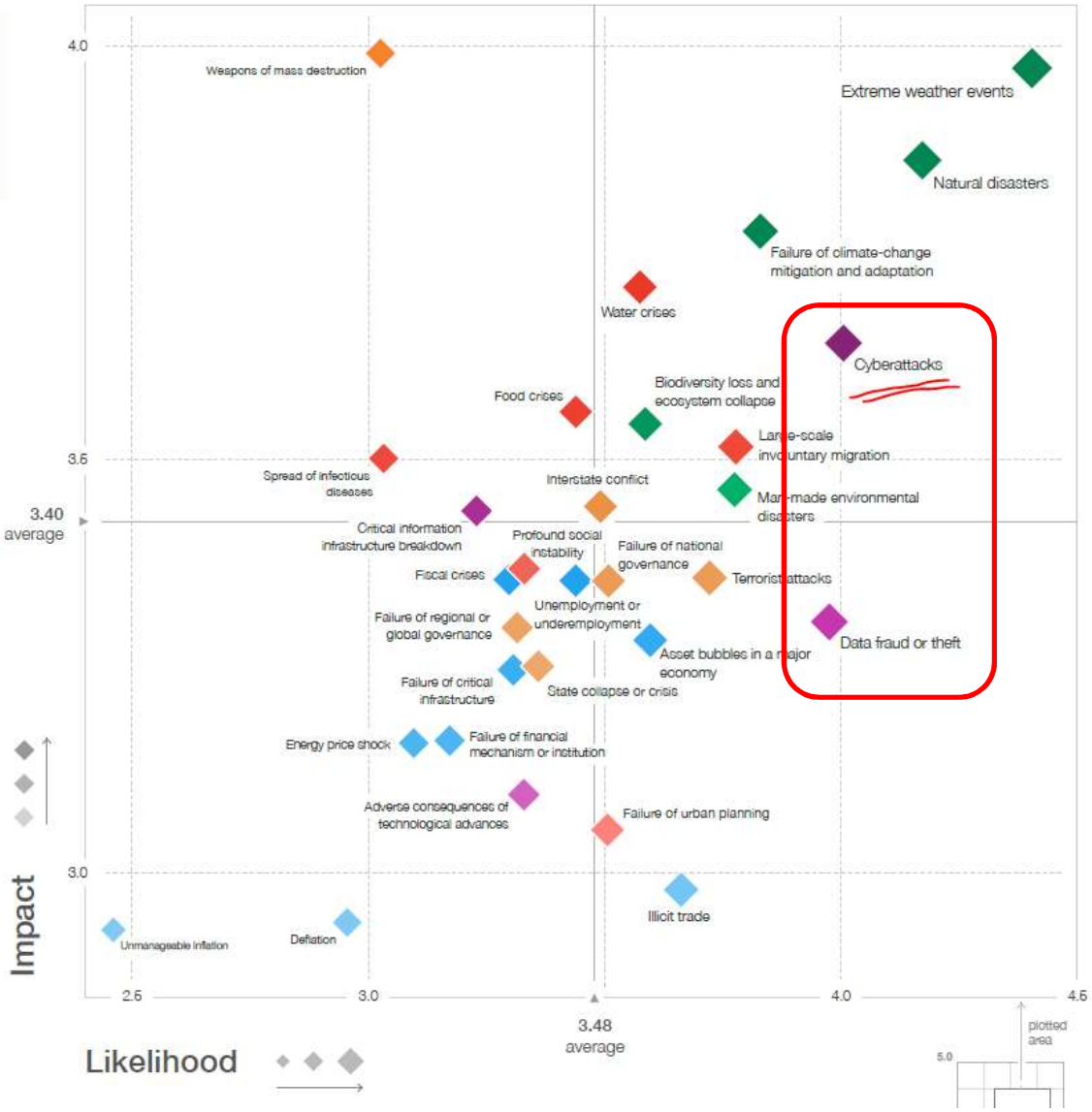
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2018
13th Edition

Figure I: The Global Risks Landscape 2018



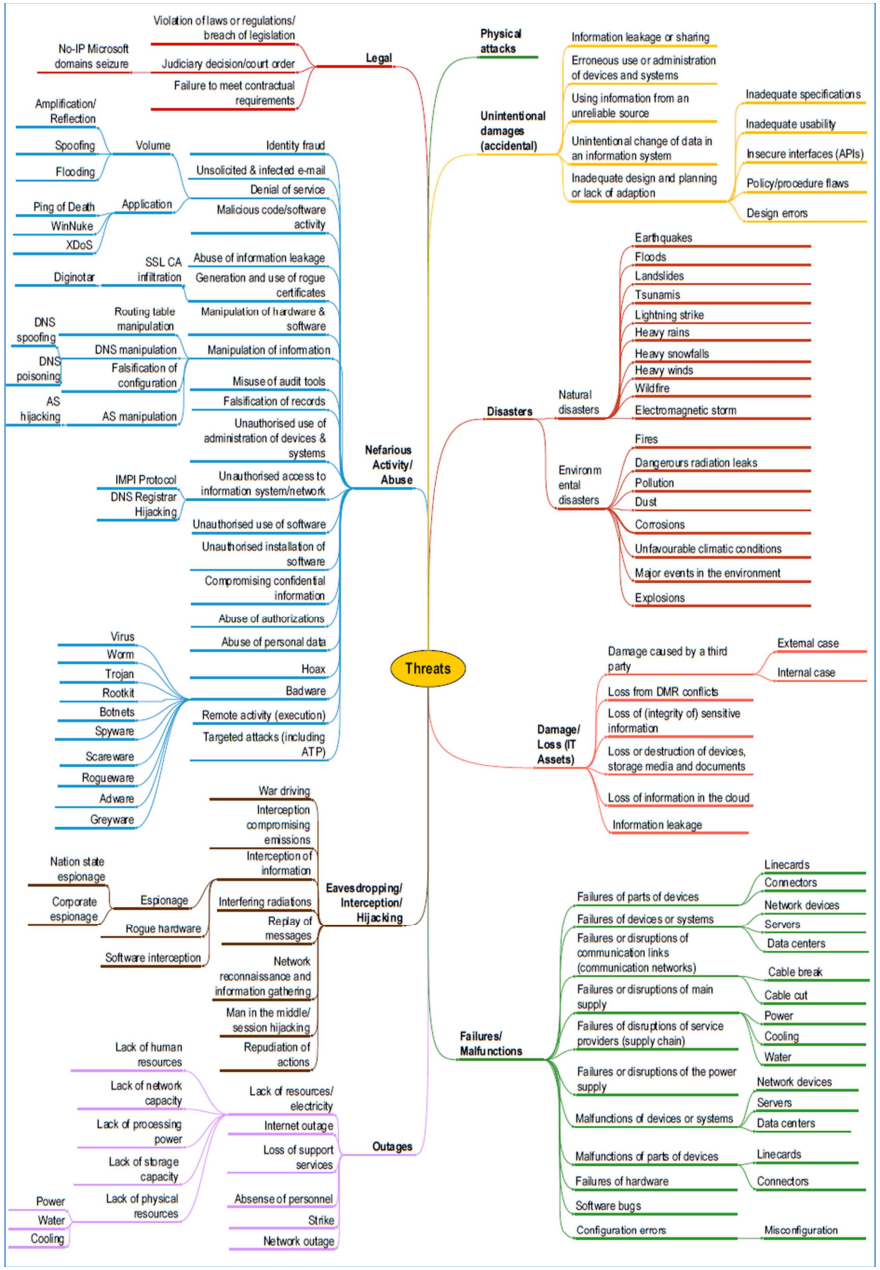
Ciber amenazas

ENISA Threat Taxonomy

A tool for structuring threat information

INITIAL VERSION
1.0
JANUARY 2016

www.enisa.europa.eu European Union Agency For Network And Information Security



Ciberseguridad: La Directiva NIS

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."

European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017

Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 6 de julio de 2016

relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

REGLAMENTO DE EJECUCIÓN (UE) 2018/151 DE LA COMISIÓN

de 30 de enero de 2018

por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo

Áreas de Acción / Respuestas

ACCIÓN:

- Normas técnicas (NIA+ISSAI)
- Guías (GPF-OCEX)
- Formación del personal actual
- Nuevos perfiles técnicos
- Equipos integrados
- Ciberseguridad
- Técnicas de análisis digital
- Técnicas de visualización
- Tecnologías cognitivas (I.A.)
- Auditoría de sistemas

Reingeniería de procesos

"Los retos del futuro inmediato (cambios disruptivos tecnológicos, entre otros) exigen de la profesión una ***respuesta proactiva****."*

"La transformación también exigirá la adquisición de nuevas áreas de conocimiento, así como la incorporación ineludible de sistemas inteligentes en los procesos (Big Data analytics, programas predictivos y soluciones de ciberseguridad)."

Daniel Faura
10/10/2016

2005

2018

Plan Estratégico 2019-2021

Nuevas guías de auditoría (ASOCEX)

ISSAI 5300

INTOSAI

Directrices sobre Auditoría de TI

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5300: **Directrices de auditoría de tecnologías de la Información**

Referencia: ISSAI 5300 Directrices sobre auditoría de TI, aprobada en el XXII INCOSAI, en diciembre de 2016

MANUAL DE LA IDI Y DEL WGITA SOBRE AUDITORÍA DE TI PARA LAS ENTIDADES FISCALIZADORAS SUPERIORES

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1316: El conocimiento requerido del control interno de la entidad

NIA315

ANEXO 1: **Análisis del control interno en un entorno informatizado**

(Manual de procedimientos de fiscalización de regularidad del Tribunal de Cuentas, apartado 5.3)

La revisión de
la actividad fi

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1500: Evidencia de auditoría

NIA500

Anexo 2 Consideraciones sobre la **evidencia electrónica de auditoría**

"Las tecnologías emergentes y los retos que presenta a las organizaciones, ofrece muchas posibilidades a la profesión auditora.

*En los próximos años deberemos **adaptarnos** a una revolución tecnológica, aprovechar la inteligencia artificial y elaborar **guías de auditoria** relacionadas con la ciberseguridad".*

Olivia Kirley,
Presidenta de IFAC

23/8/2016

Nuevas guías de auditoría (ASOCEX)

Guía práctica de fiscalización de los OCEX Draft

GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica

Refe[illegible]

Borrad

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5340: Los controles de aplicación: qué son y cómo revisarlos Draft

Referencia: ISSAI-ES 5300, GPF-OCEX 5000 y GPF-OCEX 1315

Borrador elabo

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5370 Guía para la realización de pruebas de datos Draft

Referencia:

Borrador de 01,

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

Referencia: GPF-OCEX 1315, 1500 y 5300

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 27/11/2017

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5313 Revisión básica de ciberseguridad Draft

Referencia: GPF-OCEX 5311, Esquema Nacional de Seguridad, CIS Controls IS Audit/Assurance Program de ISACA, CIS Controls.

Nuevos perfiles del auditor público

Personal y equipos especializados en:

- Auditoría de sistemas informatizados.
- Análisis de Datos, Big Data y Cloud.
- Herramientas de análisis de datos y de visualización.
- Ciberseguridad.

Auditores en general:

- Deberán tener un nivel alto de conocimientos tecnológicos, más profundo que el existente actualmente.
- Se deberán establecer acciones formativas orientadas a las nuevas necesidades, dirigidas a los actuales y futuros profesionales.

*"**Un nuevo tipo de auditoría requiere un nuevo tipo de auditor**.*

Seguirá siendo esencial que el auditor tenga un sólido conocimiento de los fundamentos de la auditoría.

Pero se necesitarán una variedad de conocimientos avanzados, incluyendo la utilización de herramientas de análisis de datos."

Thomas Davenport

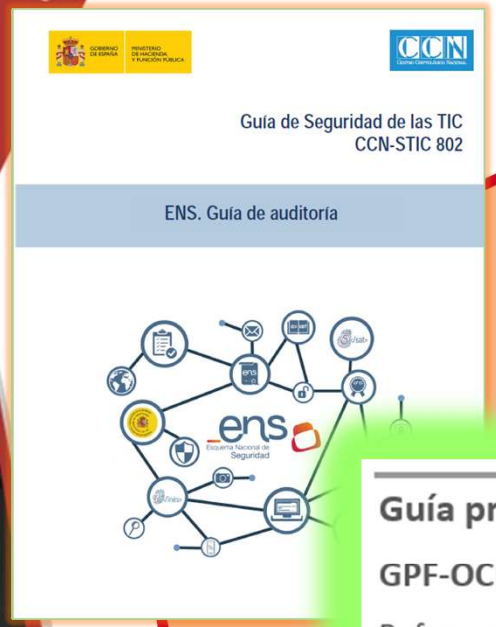
2016

E-administración y la evidencia electrónica

La información y los datos que circulan, almacenan o se procesan en un sistema de información deben tener una serie de características **(disponibilidad, autenticidad, integridad o confidencialidad)** que los controles de seguridad deben garantizar, tal como requiere la Directiva de Ciberseguridad.

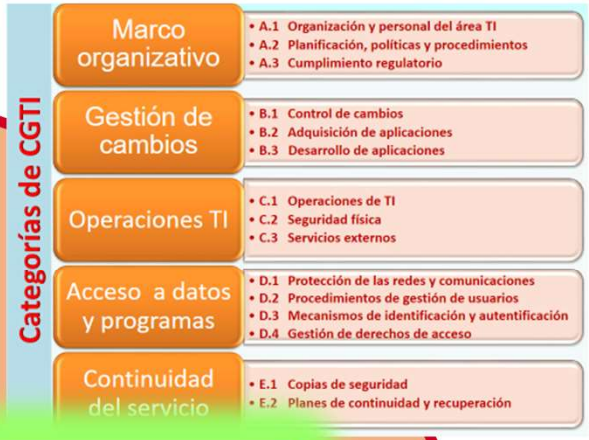
Los auditores externos deben revisar los controles internos diseñados e implantados en los sistemas de información para garantizar que los datos utilizados como fuente de evidencia tienen esas características.

Ciberseguridad: Nueva GPF-OCEX 5311



enisa

CIS Critical Security Controls



Guía práctica de fiscalización de los OCEX

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

Referencia: GPF-OCEX 1315, 1500 y 5300

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 27/11/2017

CCN Centro Criptológico Nacional

El objetivo de esta guía es servir de introducción a la problemática que la ciberseguridad plantea en la actividad de los auditores de los OCEX, concienciar sobre su importancia y señalar algunas líneas de desarrollo posterior de las GPF-OCEX.

Enfoques principales de una auditoría de Ciberseguridad

- Realizar una **auditoría de ciberseguridad** consistente en un análisis a fondo de la cuestión en un determinado ente.

  Podría ser similar a una auditoría de seguridad de las requeridas por el ENS o una auditoría siguiendo la metodología de ISACA.

  Un trabajo de este tipo entraña una intensa dedicación de personal especializado tanto para el auditor como para el ente auditado.

- La revisión de aspectos directamente relacionados con las áreas significativas auditadas en una **auditoría financiera**.

  Consistirá en la revisión de los **CGTI** relacionados únicamente con las áreas significativas del ente auditado para los fines de la auditoría financiera. **>>>> GPF-OCEX 5330**

- La revisión de una serie de **controles básicos de ciberseguridad**.

  Permitirá formar una idea general de la situación en la entidad revisada y no requiere la dedicación de excesivos recursos especializados ni al auditor externo ni al ente auditado. **>>>> GPF-OCEX 5313**

Auditoría de los CGTI

- Ley
- Reglamento
- ISSAI-ES: Principios fundamentales de la fiscalización
- Principios y normas de auditoría
- Declaración de Pamplona
- Manual de fiscalización 2017
- Manual de fiscalización 2018
- Políticas generales de gestión y seguridad de los SI

web sindicatura / normativa / manual de fiscalización 2018

MANUAL DE FISCALIZACIÓN 2018

Revisión CGTI	2850		
Revisión CGTI nivel básico	2857		
Revisión CGTI nivel básico. Cuestionario	2857.1		
Revisión CGTI nivel medio	2858		
Revisión CGTI nivel medio. Formulario	2858.1		
Revisión CGTI nivel alto	2859		
Revisión CGTI nivel alto. Cuestionario	2859.1		
Guía de fiscalización de área de gastos de personal	2861		
Documentar la comprensión del proceso de gestión de personal-nóminas	2861.1		
Guía de fiscalización del área de compras, gastos y proveedores	2862		

OCEX

GPF-OCEX 5330

GPF-OCEX 5330 Draft

CGTI

Marco organizativo

- A.1 Organización y personal del área TI
- A.2 Estrategia
- A.3 Políticas y procedimientos
- A.3 Cumplimiento normativo

Gestión de cambios

- B.1 Adquisición de aplicaciones y sist.
- B.2 Desarrollo interno de aplicaciones
- B.3 Control de cambios

Operaciones TI

- **C.1 Inventario hardware y soft.**
- C.2 Proc. Control activ.
- **C.3 Gestión incidentes**
- C.4 Antivirus
- C.5 Seguridad Física
- C.6 Servicios Externos
- **C.7 Configuraciones Seguras**
- **C.8 Monitorización Audit Logs**

Acceso a datos y programas

- D.1 Protección de las redes y comunicaciones
- D.2 Procedimientos de gestión de usuarios
- D.3 Mecanismos de identificación y autenticación de usuarios
- **D.4 Control sobre privilegios administrativos**

Continuidad del servicio

- E.1 Copias de seguridad
- E.2 Planes de continuidad y recuperación

Auditoría de ciberseguridad

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Pruebas de auditoría sobre ciberseguridad

Ejemplo CIS 4, Control sobre privilegios administrativos

- Verificar que existe un procedimiento que garantice que se restrinjan los permisos de administración a los casos en que sea necesario y que sólo se utilicen las cuentas de administrador cuando sea necesario

- Verificar si se registra la actividad de los usuarios administradores y se revisa.

- Revisar las listas de usuarios con acceso privilegiado y comprobar si el número de usuarios es el apropiado. Comprobar que el acceso es el apropiado en base a las funciones del puesto de trabajo.

Objetivos de la revisión básica de ciberseguridad

- Verificar que las entidades auditadas tienen un grado de resiliencia frente a las ciber amenazas adecuado a los servicios que prestan

- Mejorar la eficacia de los controles de ciberseguridad en las entidades auditadas

Seguridad de la información: se recoge en la nueva Ley de Sindicatura de Cuentas

DIARI OFICIAL
DE LA GENERALITAT VALENCIANA

Legislación consolidada

Última revisión 13.12.2017

Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Cu

… use of electronic tools …

… granted access to electronic data bases …

To verify the **security and reliability of computer systems** that support the financial information, accounting and management information.

Artículo 7. Función fiscalizadora

El ejercicio de la función fiscalizadora la realizará la Sindicatura de Comptes por los siguientes medios:

..

c) Para el desarrollo de sus funciones, la Sindicatura de Comptes podrá utilizar todos los medios adecuados para la consecución de sus objetivos, incluidos los de carácter informático y la contratación de expertos. El Consejo también podrá contratar con empresas consultoras o de auditoría para el cumplimiento de su programa anual de actuación.

Artículo 11. Medios de información para el ejercicio de la función fiscalizadora y consecuencias derivadas de la obstrucción al ejercicio de la actividad fiscalizadora

Uno. En el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para:

a) Acceder a todos los expedientes y documentos de cualquier clase relativos a la gestión del sector público valenciano, incluyendo las bases de datos electrónicas en las que se archiven, así como para pedir, a los que estén sometidos a su control, cuantos escritos, informes o aclaraciones orales considere necesarios.

..

c) Efectuar las comprobaciones que considere oportunas en relación con los activos, pasivos, transacciones, procesos, control interno, etcétera.

d) Verificar la seguridad y fiabilidad de los sistemas informáticos que soportan la información económico-financiera, contable y de gestión.

Moltes gràcies!