ISACA
Trust in, and value from, information systems
Barcelona Chapter


# Sesión 4 – LA SEGURIDAD DE LA INFORMACIÓN

Joaquim Altafaja Diví, CISA, CISM, CGEIT
VP ISACA Barcelona Chapter

ISACA
Trust in, and value from, information systems
Barcelona Chapter

- **Fundada en 1969**
- Desde 1978, **CISA** ha sido aceptado globalmente como un estándar de competencia sobre la auditoría de TI, control y los profesionales de seguridad
- Más de 140.000 miembros en 180 países
- Más de 215 capítulos alrededor del mundo
- IT Governance Institute (ITGI) fue creado por ISACA en 1998
- COBIT5 es la última edición del globalmente aceptado **Marco** de Gobierno de TI de ISACA

# ISACA: Visión y Misión

## Visión ISACA

"Confianza y valor desde, de los sistemas de información"

## Misión ISACA

"Para profesionales y organizaciones, siendo el proveedor global líder en conocimiento, certificaciones, comunidad, tutela y educación sobre los sistemas de información, auditoria y seguridad, gobernanza de TI, riesgos de TI y *cumplimiento*"

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# ISACA Certificaciones

## Programas CISA/CISM/CGEIT/CRISC

### Certified Information Systems Auditor (CISA)
Más de 130.000 certificados desde 1978


### Certified Information Security Manager (CISM)
Más de 34.000 certificados desde 2002


### Certified in the Governance of Enterprise (CGEIT)
Más de 7.000 certificados desde 2007


### Certified in Risk and Information Systems Control
Más de 20.000 certificados desde 2010

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Acreditación ANSI

- American National Standards Institute (ANSI) ha otorgado la acreditación **ISO/IEC 17024:2012** a los programas de Certificación **CISA**, **CISM**, **CGEIT** y **CRISC**.

- **Ser acreditados por** ANSI significa que los procedimientos de ISACA satisfacen los requisitos esenciales de **transparencia, equilibrio, consenso y procedimiento debido.**

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# ISACA Productos y Servicios

## Productos CSX/COBIT/CMMI

### Cybersecurity Nexus

Divulgar conocimientos sobre Ciberseguridad
Provee conocimiento y habilidades basadas en evaluaciones

CSX CYBERSECURITY NEXUS

### COBIT 5

Marco de gobierno eficaz de los sistemas digitales de hoy
y las tecnologías emergentes del mañana.
Ha sido referencia para el gobierno y la gestión de TI

COBIT 5

### CMMI

En 2016, ISACA adquirió el Instituto CMMI de la Universidad Carnegie Mellon.
Las evaluaciones de CMMI permiten a las empresas medir su capacidad y
madurez frente a un marco definido de mejores prácticas
e identificar las áreas en las que ser más competitivas

CMMI

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# ¿Por qué Certificaciones ISACA?

- ***Conocimiento y habilidades mejoradas***
  - Para demostrar la buena disposición a mejorar los conocimientos técnicos y habilidades.
  - Para demostrar a la gerencia su competencia y responsabilidad hacia la excelencia organizacional.

- ***Avance en la carrera profesional***
  - Para obtener credenciales que los empleadores buscan.
  - Para mejorar su imagen profesional.

- ***Reconocimiento Mundial***
  - Para ser relacionado con los más de 140,000 profesionales que han conseguido la designación **CISA, CISM, CGEIT, CRISC**

ISACA
Trust in, and value from, information systems
Barcelona Chapter

¿Desea conocer más?

**ISACA Barcelona Chapter**
Plaça Ramón Berenguer el Gran, 1

- +34 672 365 424
- E-mail: info@isacabcn.org

www.isacabcn.org

www.isaca.org

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Control Interno

- Relación directa entre
  - Control Interno
  - Seguridad de la Información

✓ Los sistemas de información están absolutamente implicados en la obtención o emisión de la información financiera de las entidades

✓ Contribuir a la mejora del escenario de la auditoría financiera

✓ La aplicación de las NIA adaptadas, si bien enfocadas a regular el marco general, lo que implica una mayor aplicación del juicio profesional del auditor de cuentas en su interpretación, supone que el auditor debe llevar a cabo un **análisis del control interno en entornos informatizados**

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Seguridad de la Información

- Figuras de la continuidad de negocio

  - ✓**BIA (Business Impact Analysis)**
  - ✓**BCP (Business Continuity Planning)**
  - ✓**DR (Disaster Recovery)**
  - ✓**BRP (Business Recovery Plan)**
  - ✓**PDS (Plan Director de Seguridad)**
  - ✓**RTO (Tiempo Objetivo de Recuperación)**
  - ✓**RPO (Punto Objetivo de Recuperación)**

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Seguridad de la Información

## CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD


La **confidencialidad** es la protección de la información contra el acceso no autorizado o la divulgación.

La **integridad** es la protección de la información contra la modificación no autorizada (El concepto de integridad también se aplica a software y configuraciones)

La **disponibilidad** garantiza el acceso oportuno y confiable al uso de la información y los sistemas

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# CIBERSEGURIDAD *vs* SEGURIDAD DE LA INFORMACIÓN

La **seguridad de la información** trata de la información, independientemente de su formato Incluye:

- Documentos en papel
- Propiedad digital e intelectual
- Comunicaciones verbales o visuales

La **ciberseguridad** se ocupa de la protección de los activos de información al abordar las amenazas de la información procesada, almacenada y transportada por sistemas de información **interconectados**.

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Ciberseguridad

**Los 10 delitos que marcarán la ciberseguridad en 2017 (Fuente: Diario La Ley)**

- **1. *Ransomware:* el *malware* más rentable**
- **2. Infecciones de malware sin necesidad de descargar archivos**
- **3. Ataques DDoS en servidores y sistemas Web globales**
- **4. Tráfico HTTPs malicioso: protocolos cifrados como señuelo**
- **5. *Maladvertising:* malware disfrazado de publicidad**
- **6. *Phishing-spearphishing* más realista y verosímil**
- **7. Fraude en el "mundo real" para acceder a información digital**
- **8. Móviles y la información en la nube**
- **9. Más puntos de ataque con la incorporación del Internet de las Cosas**
- **10. La inteligencia artificial entra en los objetivos de los ciberatacantes**

## Factores de negocio y entorno empresarial a considerar

- Naturaleza del negocio
- Tolerancia al riesgo
- Perfil de seguridad
- Tendencias de la industria para la seguridad
- Fusiones, adquisiciones y alianzas (integración)
- Servicios externalizados

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Ciberseguridad

## Consecuencias de un impacto de ciberseguridad

- Pérdida de información
- Interrupción de actividades
- Pérdida de ingresos
- Daños a equipos informáticos
- Daño reputacional
- Enfrentarse a acciones legales

# Enfoques en ciberseguridad

**En general, hay tres enfoques diferentes para la implementación de la ciberseguridad**

• **Basado en cumplimientos** —También conocido como la seguridad basada en estándares, este enfoque se basa en reglamentos o normas para determinar las implementaciones de seguridad. Los controles se aplican con independencia de su aplicabilidad o necesidad, lo cual a menudo conduce a una actitud de llevar "lista de control" hacia la seguridad

• **Basado en riesgos** —La seguridad basada en riesgos se basa en identificar el riesgo único al que una organización en particular se enfrenta y el diseño e implementación de los controles de seguridad para hacer frente a ese riesgo por encima y más allá de la tolerancia al riesgo y de las necesidades de negocio de dicha organización

• ***Ad hoc*** —Un enfoque *ad hoc,* simplemente implementa la seguridad sin fundamento o criterio particular. Las implementaciones ad hoc pueden ser impulsadas por la comercialización del proveedor, o pueden reflejar insuficiente experiencia en la materia, conocimiento o capacitación en el diseño y aplicación de salvaguardas

# Wanna Cry, Golden Eye/Petya … y seguirá

## Lecciones que debemos aprender

- Identificar el vector de ataque


- Mantener el sistema operativo y el antivirus actualizados
- No abrir ficheros, adjuntos o enlaces de correos electrónicos no confiables, ni contestar a este tipo de correos.
- Precaución al seguir enlaces en correos, mensajería instantánea y redes sociales, aunque sean de contactos conocidos.
- Ante la menor duda BORRAR el correo y llamar por teléfono al remitente para que confirme origen y contenido.
- Informar a todo el personal de estas recomendaciones

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Ciberseguridad

**La ciberseguridad se transforma en un elemento material más de la auditoría de cuentas por los efectos sobre el negocio, las posibles implicaciones legales y se postula como un indicador de la preparación de la organización para abordar el futuro**

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# Auditoría 4.0 ?

## Industria 4.0, Sociedad 4.0

- CAATs (Computer Assisted Audit Techniques)
- Revolución de los datos (impacto de los datos y utilizarlos como palanca impulsora del negocio)
- Big Data, BI, AI, …
- Cambios en la forma de auditar (Ej. SII)
- La veracidad de los datos entra en escena

# Blockchain

- Blockchain = Fin de los datos centralizados
- La transacción no requiere de intermediario centralizado que identifique y certifique la información
- No puede ser borrada
- La red de nodos distribuidos certifican la autenticidad de los datos, confidencialidad, integridad, disponibilidad y **veracidad**
- Realización de transacciones entre partes de manera segura, confiable e irreversible, sin necesidad de intermediario para establecer una relación de confianza entre las partes
- Smart Contract, acuerdos sin revelación de información confidencial. Fin de la información privilegiada.
- Transacciones públicas o privadas dependiendo del propósito
- Transparencia en base a quienes estén autorizados para obtener acceso

ISACA
Trust in, and value from, information systems
Barcelona Chapter

# GRACIAS

Joaquim Altafaja – VP ISACA Barcelona Chapter
joaquim.altafaja@itadvisory.es