AUDITORES

AGRUPACIÓN DE MADRID
INSTITUTO DE CENSORES JURADOS
DE CUENTAS DE ESPAÑA

XXI Día del Auditor
20 de noviembre de 2017

La importancia de la Ciberseguridad en la Auditoría Financiera

Ricardo Barrasa García
Presidente de ISACA Madrid

¿Qué es ISACA?

ISACA®

Trust in, and value from, information systems

SISTEMAS VALIOSOS Y CONFIABLES

50 ISACA

Desde 1969

217 capítulos en 188 países

150.000 Asociad@s

CISA Certified Information Systems Auditor® An ISACA® Certification

CISM Certified Information Security Manager® An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT® An ISACA® Certification

CRISC Certified in Risk and Information Systems Control™ An ISACA® Certification

CSX™ CYBERSECURITY NEXUS

COBIT® 5 AN ISACA® FRAMEWORK

ISACA en España

WWW.ISACAMADRID.ES

Madrid - 1.100

Barcelona - 400

Valencia - 150

CISA Certified Information Systems Auditor — An ISACA Certification

CISM Certified Information Security Manager — An ISACA Certification

CGEIT Certified in the Governance of Enterprise IT — An ISACA Certification

CRISC Certified in Risk and Information Systems Control — An ISACA Certification

CSX CYBERSECURITY NEXUS

COBIT 5 AN ISACA® FRAMEWORK

Marco de Referencia

- COBIT 5 (emitido por Comité directivo de COBIT y el IT *Governance Institute*) está elaborado como un estándar generalmente aplicado y aceptado sobre las políticas de seguridad y los controles sobre Sistemas de Información, y proporciona un marco de referencia universal para su desarrollo. Controla 37 procesos de TI que se traducen en mas de 200 objetivos de control
- COBIT está alineado con COSO (*desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude*) y recoge como objetivos de control:
  - La efectividad y la eficiencia de las operaciones;
  - La confidencialidad e integridad de la información financiera y
  - El cumplimiento de las leyes y regulaciones en materia de Auditoría de Sistemas de Información.
- Existe una guía profesional de orientación de COBIT 5 para la Seguridad de la Información

La seguridad de la Información

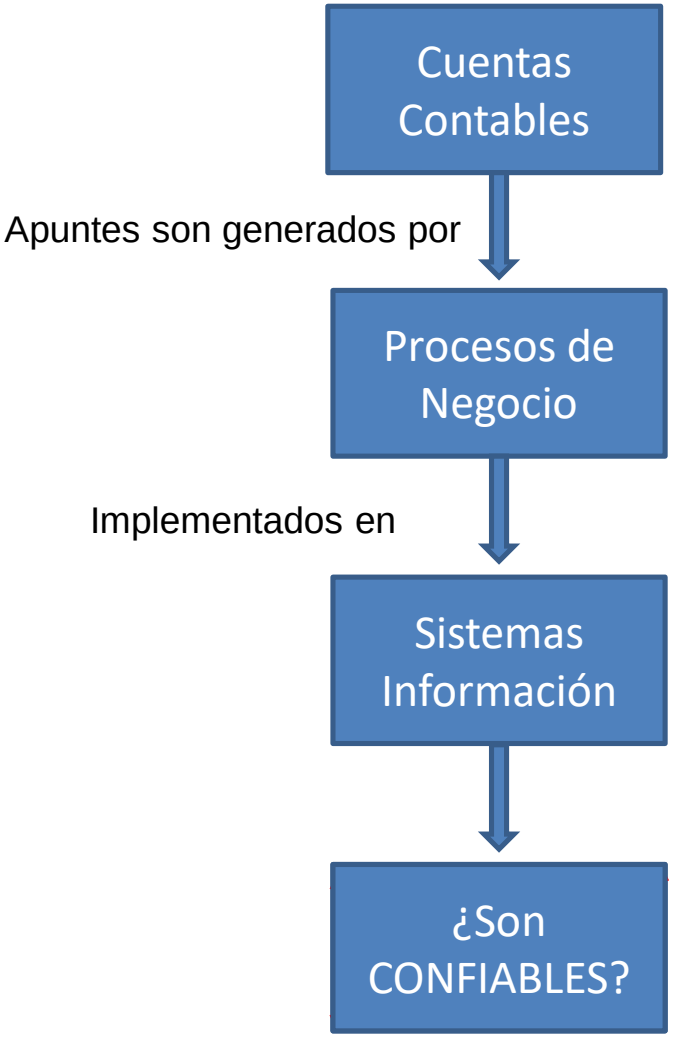
La información constituye uno de los activos más importantes de cualquier organización, independientemente de su tamaño o actividad.

Para ello tenemos que implantar medidas preventivas y reactivas en nuestras empresas, destinadas preservar y proteger la **confidencialidad,** la **disponibilidad** e **integridad** de la información.

Estas medidas serán proporcionales a la criticidad de la información que manejemos, por ello será importante **identificarla** y **clasificarla**. Las medidas también serán acordes a los sistemas a proteger, la información que contienen, las condiciones particulares de cada emplazamiento y las amenazas a las que se exponen.

Fuente: INCIBE

Reporte Financiero



Sistemas Confiables

Para determinar si un sistema es *aceptablemente* confiable, debe de cumplir unos determinados **objetivos de control**:

- Desarrollo de Sistemas
- Seguridad Lógica
- Seguridad Física
- Explotación de Sistemas

Desarrollo de Sistemas

Objetivos de control:

- Metodología de desarrollo y mantenimiento de sistemas
- Iniciación de proyectos
- Toma de requisitos del sistema
- Diseño detallado
- Pruebas de aplicaciones
- Paso a Producción
- Licencias de uso

Aplicables a la infraestructura de TI:

- Aplicación,
- Base de Datos y
- Sistema Operativo

Los riesgos que cubren estos objetivos son:

- Acceso/ alteración indebida de programas fuentes.
- Implementación injustificada de cambios.
- Desarrollos no alineados a los estándares.
- Programas productivos con funcionalidad no probada.
- Infracciones por derechos de propiedad intelectual.

Seguridad Lógica (I)

Objetivos de control:

- Control de accesos sobre los programas.
- Las aplicaciones de usuarios y el control sobre la manipulación.
- El acceso a los datos.
- El control sobre el acceso a bases de datos productivas.

Aplicables a la infraestructura de TI:

- Aplicación,
- Base de Datos y
- Sistema Operativo

Los riesgos que cubren estos objetivos son:

- Robo/ extracción de datos.
- Retrasos para la restauración de las operaciones.
- Accesos no autorizados al sistema.
- Incidentes de seguridad sobre activos informáticos.
- Vulnerabilidades de seguridad en el software.
- Usuarios con privilegios indebidos sobre el sistema.

……

Seguridad Lógica (II)

Objetivos de control:

- Control de accesos sobre los programas.
- Las aplicaciones de usuarios y el control sobre la manipulación.
- El acceso a los datos.
- El control sobre el acceso a bases de datos productivas.

Aplicables a la infraestructura de TI:

- Aplicación,
- Base de Datos y
- Sistema Operativo

Los riesgos que cubren estos objetivos son:

……

- Accesos lógicos no autorizados al sistema operativo.
- Accesos a archivos con información sensible.
- Utilización de servicios no seguros.
- Vínculos entre instalaciones operativas y de desarrollo.
- Facilidad de adivinación de contraseñas.

Seguridad Física

Objetivos de control:

- Seguridad del Centros de Procesamiento de Datos (CPD) e instalaciones, incluyendo las medidas de protección medioambiental.
- Planes de contingencias, de recuperación ante desastres y de continuidad de los negocios en los distintos CPDS y principales instalaciones de Tecnología de la Información.

Los riesgos que cubren estos objetivos son:

- Accesos físicos no autorizados.
- Daños accidentales/ intencionales de activos informáticos.
- Valores ambientales fuera de rango
- Discontinuidad por desastres
- Retrasos para la restauración de las operaciones.

Explotación de Sistemas

Objetivos de control:

- Salvaguarda de información (Backup)
- Soporte técnico
- Tareas no programadas
- Monitoreo Intrusiones
- Gestión de incidencias

Los riesgos que cubren estos objetivos son:

- Acceso/ alteración indebida de programas fuentes.
- Implementación injustificada de cambios.
- Desarrollos no alineados a los estándares
- Programas productivos con funcionalidad no probada.
- Carencia de licencias de uso.
- Contraseñas por defecto.
- Enlaces entre instalaciones productivas y de desarrollo.
- Ausencia de trazabilidad.

Otros Sistemas/Tecnologías

- **ERP** (Enterprise Resource Planning)
  - SAP / R3
  - META 4
- Computación en la nube
  - Privada, pública o híbrida
  - Infraestructura como servicio (IaaS) se alquila infraestructura de TI
  - Plataforma como servicio (PaaS) incluye los servicios informáticos
  - Software como servicio (SaaS) hospedan y administran las aplicaciones y la infraestructura necesaria.
- Blockchain
- ….

AUDITORES

AGRUPACIÓN DE MADRID

INSTITUTO DE CENSORES JURADOS DE CUENTAS DE ESPAÑA

Gracias por su atención