Los Lunes del Instituto de Auditores Internos

#LosLunesIAI - @Auditorinterno

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del proceso de inversión en tecnologías emergentes

Eva López de Sebastián
Juan Armendáriz
Rubén de Miguel

Instituto de Auditores Internos de España

Lunes, 30 de noviembre de 2020

Transformación digital…

Comisión técnica del IAI

Cristina Fabre Chicano, *CEPSA*

Pablo Gallego Tortuero, *WIZINK BANK*

Julio Somoza Sáez, *GRUPO SANTANDER*

Yolanda Pérez Pérez, *KPMG*

Santiago Cardona Torres, *EY*

Marina Touriño Troitiño, CIA, CISA, CRMA, CPA, CISM, TEAI

Carlos Morales Luchena, *BBVA*

Juan Palomo Cisneros, *DELOITTE*

Juan Armendáriz Vergarajáuregui, *ALLFUNDS*

Rubén de Miguel Esteban, *MAPFRE*

Coordinación: Eva López de Sebastián Miró, *VIESGO*

Cuestiones preliminares

¿Tecnologías emergentes? ¿Alguna en concreto?

DEF: Tecnología emergente es la ciencia que se aplica a la resolución de problemas concretos que –de forma ***disruptiva****- modifica,* ***transforma****,* ***innova*** *y genera* ***nuevas oportunidades*** *en el uso de sistemas.*

¿Nuevo enfoque de Auditoría Interna? ¿Cómo aportar valor?

Enfoque tradicional, pero comprendiendo el **razonamiento estratégico**, anticipándose a los **riesgos**, planteando las **cuestiones clave** y proporcionando **información relevante a los órganos de dirección**.

Estructura del documento

Tecnologías emergentes

Inversiones y posicionamiento de Auditoría Interna

Cómo auditar los riesgos

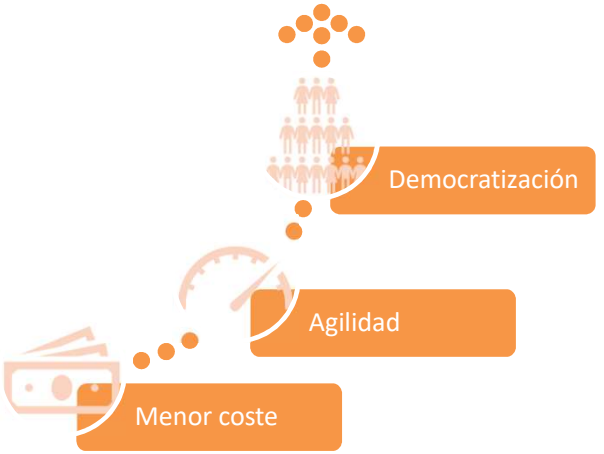
Tecnologías emergentes

Principales tecnologías emergentes

BLOCKCHAIN	CLOUD	INTELIGENCIA ARTIFICIAL	RPA	INTERNET of THINGS	BIG DATA	5G

Ciclo de vida de tecnologías emergentes

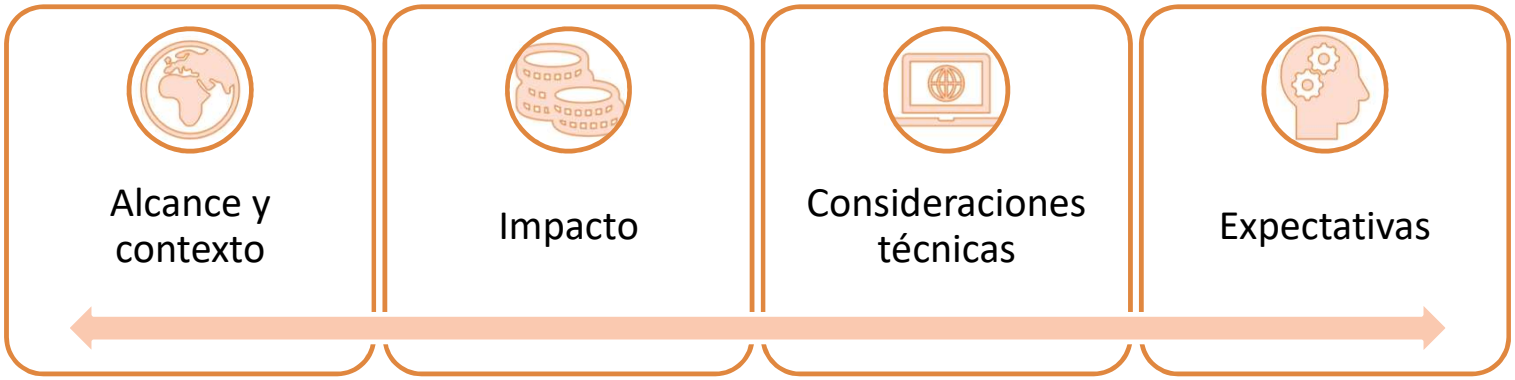
Fases del ciclo
Momentos de decisión
Evolución del ciclo de vida



Inversiones y posicionamiento de Auditoría Interna

Análisis previos a la inversión

Valorar si son completos y la plausibilidad de sus hipótesis:



Inversiones y posicionamiento de Auditoría Interna

Modelo de gobierno

- Órganos de decisión y seguimiento
- Órganos operativos y de control

Impacto de la inversión

- Uso de la tecnología
- Impactos en la organización

Inversiones y posicionamiento de Auditoría Interna

Posicionamiento y rol de Auditoría Interna

Comisión de Auditoría Interna

- Evalúa aspectos críticos de las inversiones
- Plantea cuestiones sobre Auditoría Interna

Auditoría Interna

- Plan de Auditoría Interna
- Posibles servicios de consultoría*

* Salvaguardas para preservar la independencia

Cómo auditar los riesgos

Planteamiento general

Descripción → Objetivos de control → Cómo auditarlo → Ejemplos

Riesgos

Conclusiones

Auditoría Interna debe posicionarse y aportar valor

- Conocer las tecnologías y sus características
- Evaluar la reflexión estratégica y el modelo de gobierno
- Plantear las cuestiones relevantes a los órganos de Dirección
- Auditar los riesgos

Ejemplo práctico

Desarrollos en la nube y actuaciones de Auditoria Interna

Google Cloud

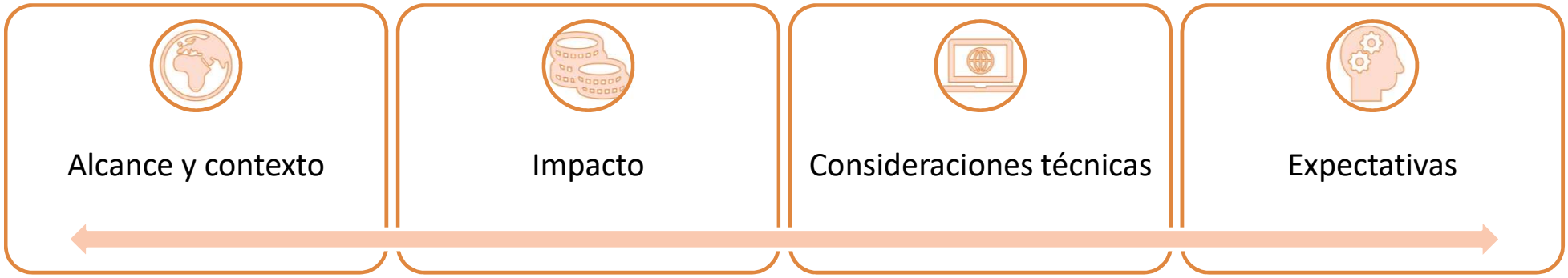
Alibaba Cloud | Worldwide Cloud Services Partner

Microsoft Azure

IBM

aws

Análisis de viabilidad



- ¿Quién va a liderar el Proyecto: IT o un área de negocio?
- Proveedor en la nube que se va a utilizar

- Dimensionamiento de recursos humanos y técnicos necesarios
- Coste de la nube: componente fijo (vs parte variable (consumo de datos)

- Obtener feedback de los departamentos internos impactados (Tecnología, Legal, Compliance, Riesgos)
- Comunicaciones, cifrado de datos y copias de seguridad

- Importante comunicar los objetivos y los posibles beneficios de forma transparente

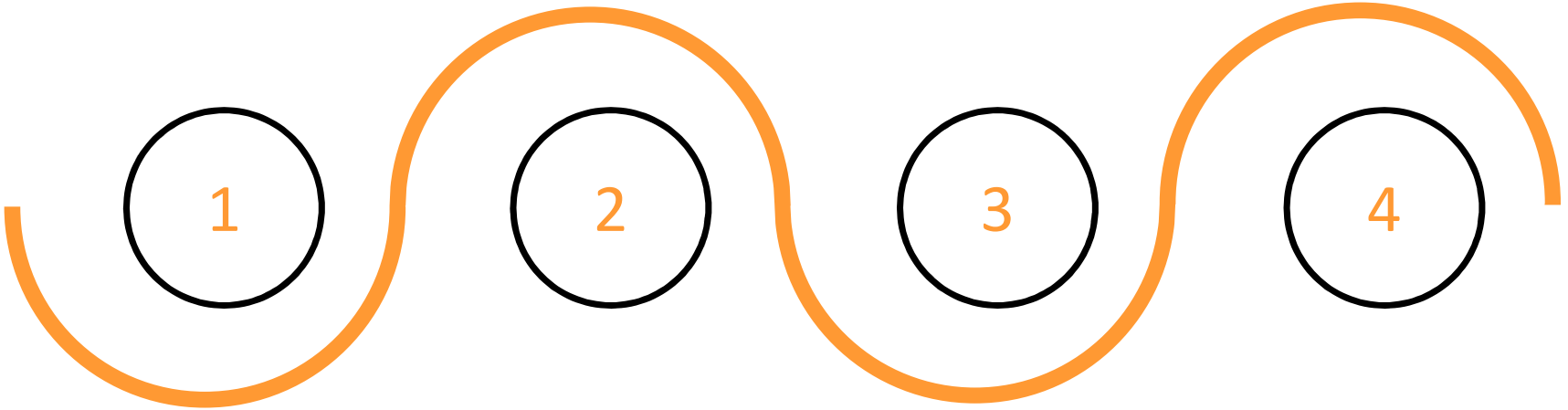
Pasos previos al desarrollo en la nube

Aprobación de la propuesta final realizada por el promotor de la iniciativa

Firma del contrato con el proveedor en la nube

Definición de niveles de acuerdo de servicio (SLAs) e indicadores de rendimiento (KPIs)

Aspectos a considerar durante el desarrollo



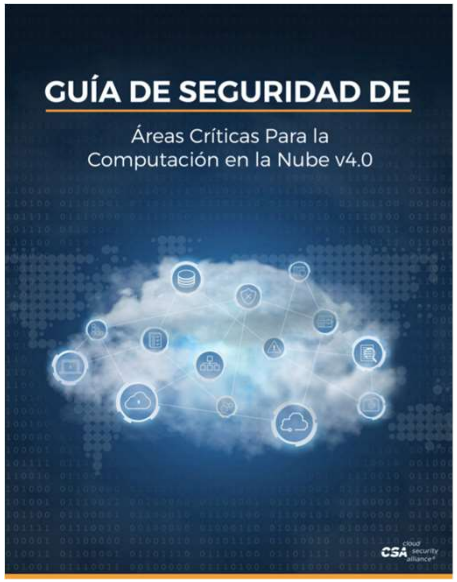
Metodología de trabajo	Documentación técnica y funcional	Seguimiento de costes	Involucración con las áreas de negocio y con Tecnología

Controles internos y seguridad de la información

- Gestión de identidades y accesos (incluido el seguimiento de super usuarios)
- Gestión de incidentes
- Ejecución de trabajos
- Plan de contingencia y copias de seguridad
- Cifrado de datos y comunicaciones (protección de datos personales)
- Gestión de cambios (existencia de una metodología), distribución de tareas y accesos a los entornos de pruebas y producción
- Revisión de los informes de auditoria facilitados por el proveedor: por ejemplo, ISAE 3402 (SOC 1) y ISAE 3000 (SOC 2)

Guías de referencia

Cloud Security Alliance (CSA)
– Guía de Seguridad de Áreas Críticas para la Computación en la Nube v4.0
– Matriz de controles esperados referenciada a la guía de seguridad emitida por CSA



Puntos clave en una auditoría Cloud

Estrategia y Modelo de Gobierno

¿Como encaja el Cloud en la estrategia de la compañía?
¿Como vamos a implantar, controlar y organizar las soluciones Cloud?

Consumo y Facturación

Pago por uso. Optimización de costes
Distribución de costes ¿Proyecto?¿Entidad?¿Elementos comunes?
Costes ocultos (ej. consumo de ancho de banda en al red)

Operación

Cambio cultural. Desarrollo y operativa para Cloud
DevOps, automatización

Seguridad y privacidad

Control de acceso. Cuentas privilegiadas. Configuración cuentas.
Conectividad con nuestros centros de datos. Modelo de Servicio
Clausulado contrato. Normativa y legislación (país, región, sector empresarial). Zonas o regiones.

Modelo de servicio Cloud

On-site	IaaS	PaaS	SaaS
Aplicaciones	Aplicaciones	Aplicaciones	Aplicaciones
Datos	Datos	Datos	Datos
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Sistema Operativo	Sistema Operativo	Sistema Operativo	Sistema Operativo
Virtualización	Virtualización	Virtualización	Virtualización
Servidores	Servidores	Servidores	Servidores
Almacenamiento	Almacenamiento	Almacenamiento	Almacenamiento
Red	Red	Red	Red

Gestionado por nosotros Gestionado por el proveedor Cloud

DISTRIBUCIÓN DE RESPONSABILIDAD

Seguridad
Privacidad de datos

TIPO de NUBE

Publica – Privada - Hibrida

RIESGO

IaaS

- Rendimiento de infraestructura depende del proveedor
- Dependencia del proveedor para cumplimiento de normativa en materia de seguridad y protección.

PaaS

- Portabilidad: dificultad para trasladar la plataforma a otros proveedores o instalaciones propias.
- Opacidad en las infraestructuras subyacentes, controladas por el proveedor íntegramente.
- Posible incumplimiento normativo de seguridad.

SaaS

- Filtración y perdida de control de datos estratégicos
- Problemas de flexibilidad en la personalización de los entornos
- Disminución de capacidad de protección y control ejercida por la organización
- Falta de estándares de portabilidad entre SaaS de diferentes proveedores
- Opacidad total en las infraestructuras
- Posible incumplimiento normativo de Seguridad

¿Como prepararnos?

FORMACIÓN

Cursos específicos / Autoformación
Experimentación
Elementos/Funciones equivalentes entre nubes

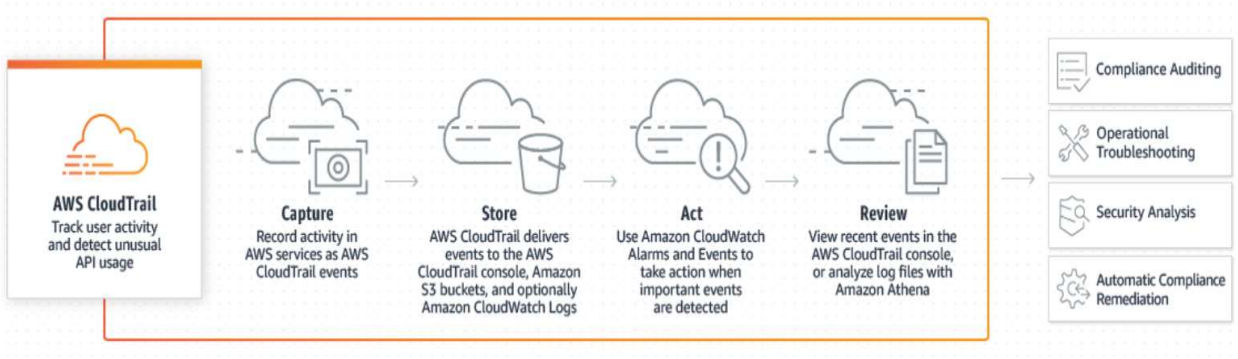
HERRAMIENTAS NATIVAS DE AUDITORÍA

Activity Log

Cloud Trail

Cloud Audit Trail

Cloud Infrastructure Audit



OTRAS HERRAMIENTAS

CloudHealth by vmware

¡¡Gracias!!

Síguenos en

www.auditoresinternos.es

@Auditorinterno

Instituto de Auditores Internos de España