"La Misión de la Auditoría Interna: Mejorar y Proteger el Valor de las Organizaciones"

16 – 19 Octubre, 2016

Instituto de Auditores Internos de la República Dominicana, Inc.
Afiliado a The Institute of Internal Auditors

FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

“Mejores Prácticas de la Auditoría de Sistemas y su Impacto en la Gestión de la Tecnología de Información”

Claudio Duran Hilario

CRMA, COBIT 5, ITIL v3, MTE, PASC

Encargado de División de Auditoría Interna de Sistemas

Superintendencia de Bancos de la República Dominicana

Sobre el conferencista

Lic. Claudio Duran Hilario

CRMA, COBIT 5, ITIL, MTE, PASC

Encargado de División de Auditoria Interna de Sistemas de la Superintendencia de Bancos

Lic. en Informática, Maestría en Tecnología Computacional, Post-Grado en Auditoría de Sistemas Computarizado, Diplomado en Hacienda Pública, Diplomado en Contabilidad Internacional, Diplomado sobre Prevención de Lavado de Activos y Financiamiento del Terrorismo Entidades Financieras, Certificación en Gestión de Infraestructura (ITIL V3 Fundation). Certificación en Gestión y Aseguramiento de Riesgos (CRMA-IIA), Certificado en COBIT 5, Encargado de División de Auditoria Interna de Sistemas de la Superintendencia de Bancos-actual. Profesor de Grado, Post-Grado y Maestría en la Universidad Autónoma de Santo Domingo (UASD), Catedrático en la Maestría Auditoría Integral y Control de Gestión, en la Universidad APEC y VALENCIA de España. Instructor de ACL, Coordinador de la Maestría en Auditoría y Seguridad Informática UASD; Actualmente Presidente del Instituto de Auditores Internos de la República Dominicana (IAIRD), miembro de ISACA y del Global IIA.

Para qué estamos aquí…

- Estamos aquí para proporcionar un amplio rango de servicios de auditoria, concebidos para ayudar a su organización a cumplir sus objetivos. Una de nuestras funciones clave es la de vigilar los riesgos y asegurar que los controles existentes sean adecuados para mitigar aquellos riesgos.
- Somos una de las piedras angulares del gobierno corporativo junto con el Consejo de Administración, la gerencia ejecutiva, y los auditores externos. Podemos ayudarle a cumplir con las nuevas legislaciones y regulaciones destinadas a mejorar el gobierno corporativo de TI. En ese orden:
  - Haremos una evaluación objetiva de sus operaciones y compartiremos ideas de mejores prácticas.
  - Brindaremos consejo para mejorar controles, procesos y procedimientos, desempeño, y gestión de riesgo.
  - Sugeriremos formas de reducir costos, mejorar ingresos e incrementar beneficios.
  - Evaluaremos los controles de aplicación de equipos, comunicaciones y softwares.

Frases comunes con respecto a la gestión de las TI

1. Customers were not happy with the inability to get to our agents and we noticed less use of our products in the marketplace.
Los clientes no estaban contentos con la incapacidad de llegar a nuestros agentes y nos dimos cuenta de un menor uso de nuestros productos en el mercado.

VP de IT - Banca / Finanzas
Problemas de Comunicación en la Red de Datos.

2. We were unable to meet an important deadline due to the server downtime. Our client was not pleased and was obligated to go with a competitor's offering at the time.
Fuimos incapaces de cumplir con un plazo importante debido al tiempo de inactividad del servidor. Nuestros clientes no estaban contentos y fueron obligados a ir con la oferta del competidor.

CIO – Manufacturing
Problemas: Infraestructura y Base de Datos-

3. We have countless internal systems. Sometimes they go off line. They can typically get the systems back on line quickly. I do not know how they are addressing the issues in the long run.
Tenemos un sinnúmero de sistemas internos. A veces están fuera de línea. Ellos pueden normalmente restablecer los sistemas de nuevo en línea rápidamente. Yo no sé cómo se están abordando los problemas en el largo plazo.
VP of Credit — Banking/Finance
Problemas: Desempeño de los Sistemas y las Redes

4. The more frequent failures are a result of server communication breakdowns, which are typically a result of overtaxing a system that is no longer adequate to support our needs. A reboot usually fixes it temporarily.

Los fallos más frecuentes son el resultado de fallas en la comunicación del servidor, que son típicamente un resultado de sobrecargar un sistema que ya no es suficiente para apoyar nuestras necesidades. Al reiniciar suele solucionar temporalmente.

SVP Corporate Mgmt. — Banking/Finance

Problema: Deficiencia en la Administración del Sistema.

5. Our main computer system (Patient Care Service) went down for almost 24 hours. Manual processes were put into action, but patient safety is at risk and routine work becomes error prone and slow.

Nuestro sistema informático principal (Servicio de cuidado al Paciente) descendió por casi 24 horas. Los procesos manuales se pusieron en acción, pero la seguridad del paciente está en riesgo y la rutina de trabajo se vuelve propensa a errores y se torna más lenta.

Problemas: Deficiencia en los Planes de Continuidad del Negocio.

Qué nos acecha…?

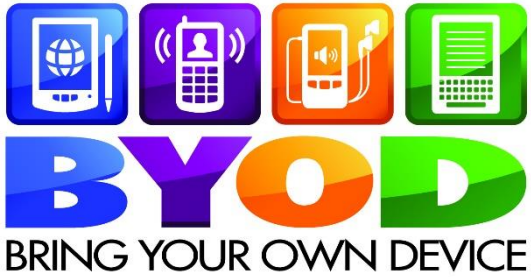
En marzo del 2014, el sitio de subastas por internet ebay, fue víctima de un **ciberataque. Los hackers** accedieron a la base de datos con la información de acceso de al menos 145 millones de usuarios.

En septiembre del año 2014, **Home Depot c**onfirmó haber sido víctima de hackers. De acuerdo con la cadena, al menos 56 millones de tarjetas de pago de clientes de tiendas en Estados Unidos y Canadá fueron afectadas. Especialistas coincidieron que los atacantes emplearon el mismo mecanismo que afectó a la cadena **Target** en 2013, cuando se descubrió un malware en las terminales de pago de sus tiendas.

Los dispositivos de Apple sufren el mayor ciberataque de su historia. Más de 50 aplicaciones para PCs, iPhone y iPads desarrolladas en China instalan un 'software' malicioso que controla los dispositivos a distancia y roba datos personales

Yahoo admite el robo de datos de 500 millones de cuentas. La empresa afirma que la información bancaria de los clientes no se ha visto afectada. Es uno de los mayores 'hackeos' de la historia.

Y que más...?: Nuevos esquemas de riesgos



La Disrupción Digital

No tiene agencia de taxis ni vehículos, pero es la mayor red de taxis del mundo.

UBER

No es una disquera musical, pero tiene el mayor repertorio de canciones de todos los géneros musicales

Spotify®

Representa la mayor red para ver películas de estrenos y no posee una cadena de cine

NETFLIX

No tiene cadena de hotel, pero es la mayor red hospedaje del mundo

airbnb

Dilemas y exigencias de las partes interesadas

- Demanda de mejores retornos de las inversiones en TI.
- Preocupación sobre el creciente nivel de gastos de TI.
- La necesidad de cumplir los requisitos regulatorios para los controles de TI.
- Incertidumbre en la selección de proveedores de servicios de TI.
- El incremento de complejidad en riesgos relacionados a TI.
- Las iniciativas de Gobierno de TI, que incluyen la adopción de marcos de referencia y mejores prácticas de control.

Estamos listos para enfrentar todo este alboroto

Dónde está el problema

Andamos así…

- **Niveles de cobertura y presencia** de Auditoría Interna de TI:
  - El 31% de las organizaciones no tiene función de Auditoría Interna de TI.
  - En el 33% de los casos sólo cuentan con 1 Auditor Interno de TI, y el 21% de las organizaciones cuenta con, al menos, entre 2 y 5 Auditores Internos de TI. Sólo el 5% tiene entre 10 y 20 Auditores Internos de TI. El 8% tiene totalmente subcontratada esta función.
  - Un 15% de las organizaciones tiene planes para incrementar el número de auditores internos de TI en el próximo ejercicio.
  - Un 56% no recurre a apoyo externo, mientras que un 44% muestra algún grado de externalización.
- **La externalización,** total o parcial, de las actividades de Auditoría Interna de TI, está motivada:
  - En el 33% de los casos por necesidades de un alto grado de especialización y actualización tecnológica.
  - En el 26% de los casos por la limitación de recursos.
- El **nivel medio de experiencia** actual de los auditores internos de TI: el 46% tienen entre 7 y 15 años de experiencia.

Importante conocer y manejar

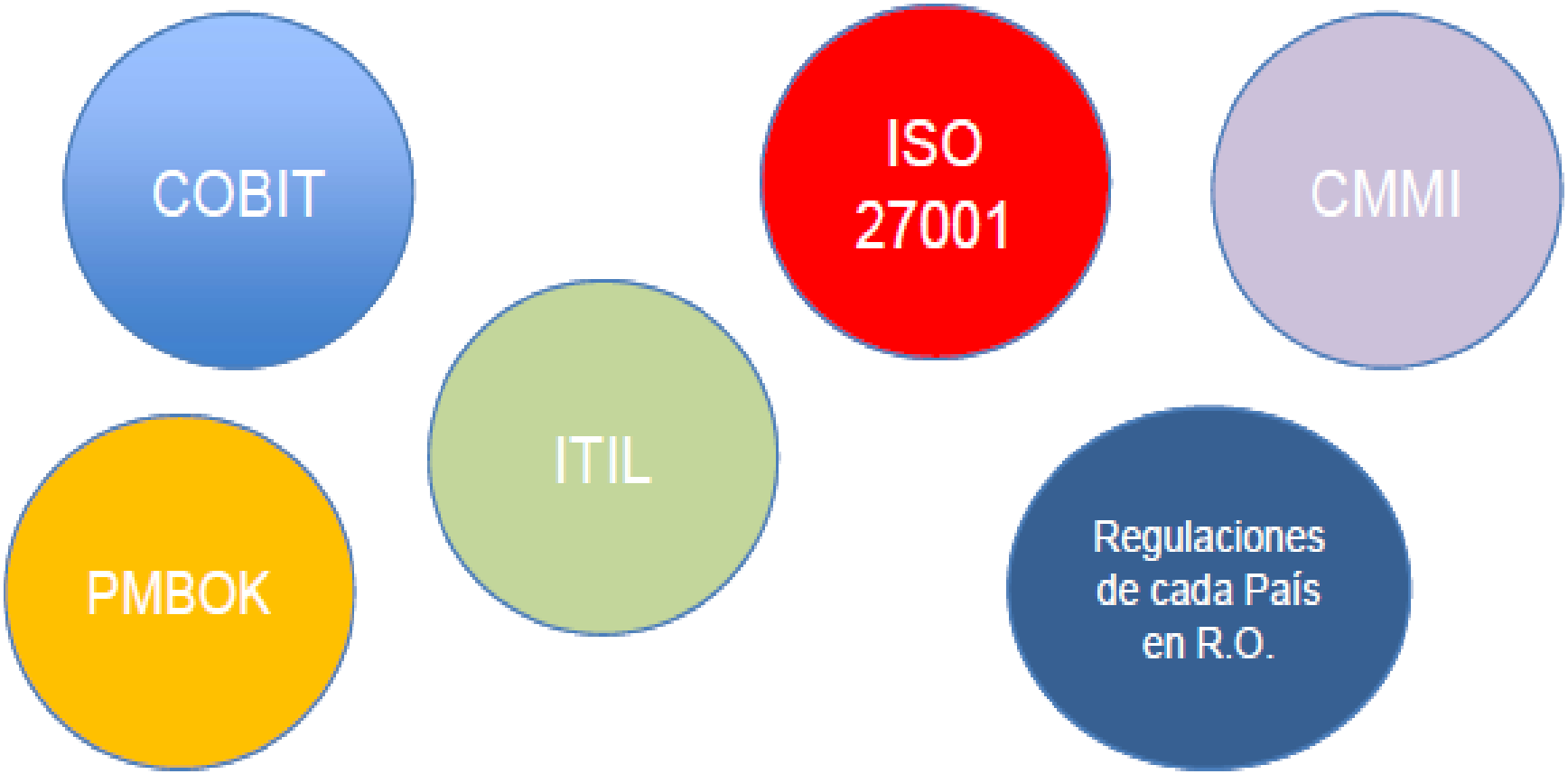
Riesgo de TI y el Riesgo Operativo

"Es el riesgo de sufrir pérdidas debido a la **no adecuación** o a **fallos** en los procesos, personal y **sistemas internos** o bien por causa de eventos externos" (BASILEA II)

Tipos de Eventos de Riesgo Operativo

- Fraude interno
- Fraude externo
- Relaciones Laborales
- Fallos en TI
- Daños (activos materiales)
- Clientes y productos
- Procesos

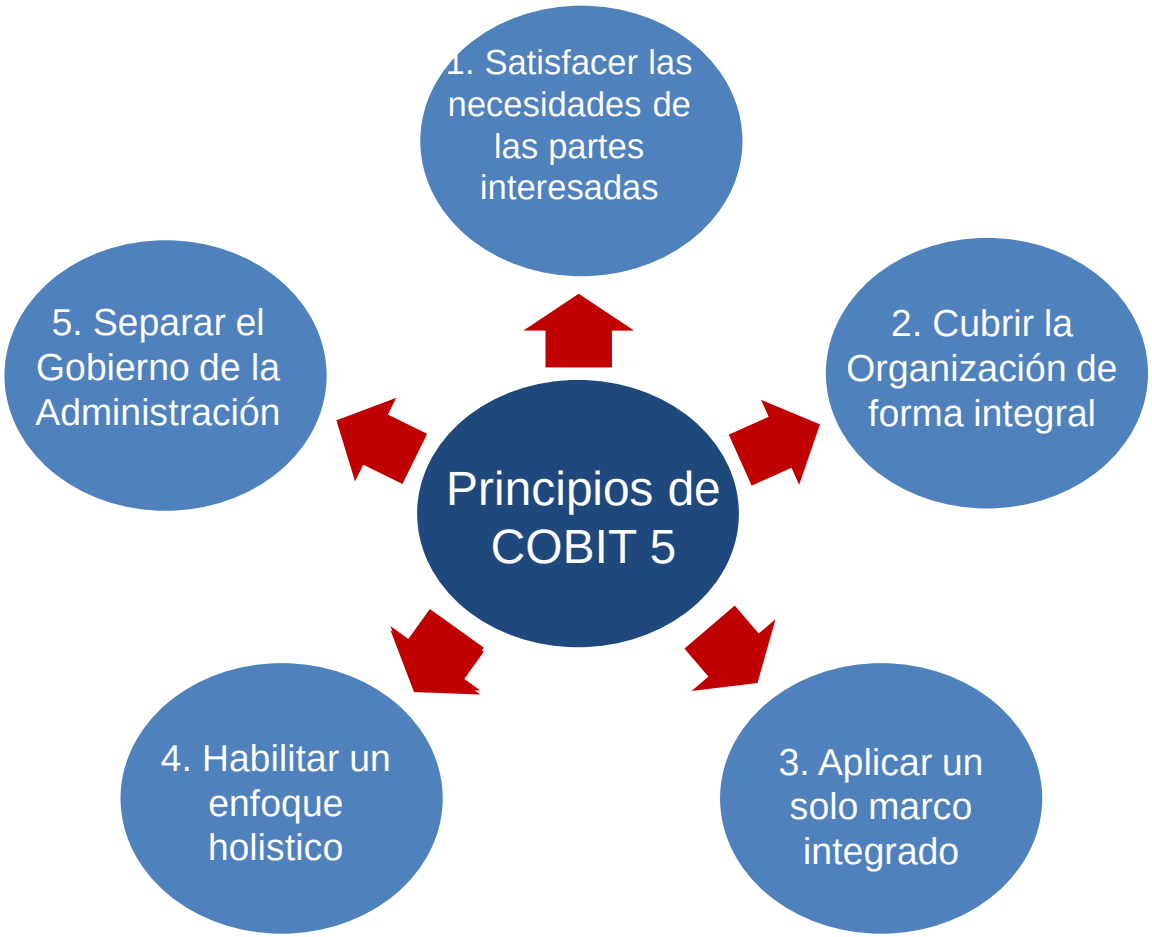
Que hacer…?


COBIT
ISO 27001
CMMI
ITIL
PMBOK
Regulaciones de cada País en R.O.

El Marco COBIT 5

Ayuda a las Organizaciones a crear un valor óptimo a partir de las TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. Permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

Los Principios de COBIT 5



COBIT 5 une los **cinco principios** que permiten a la Organización construir un marco efectivo de **Gobierno** y **Administración** basado en una serie holística de **siete habilitadores**, que optimizan la inversión en **tecnología e información** así como su uso en beneficio de las partes interesadas.

Fuente: COBIT® 5, Figura 2. © 2012 ISACA® Todos los derechos reservados.

Fuente: COBIT® 5, Figura 2. © 2012 ISACA® Todos los derechos reservados.
17

ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

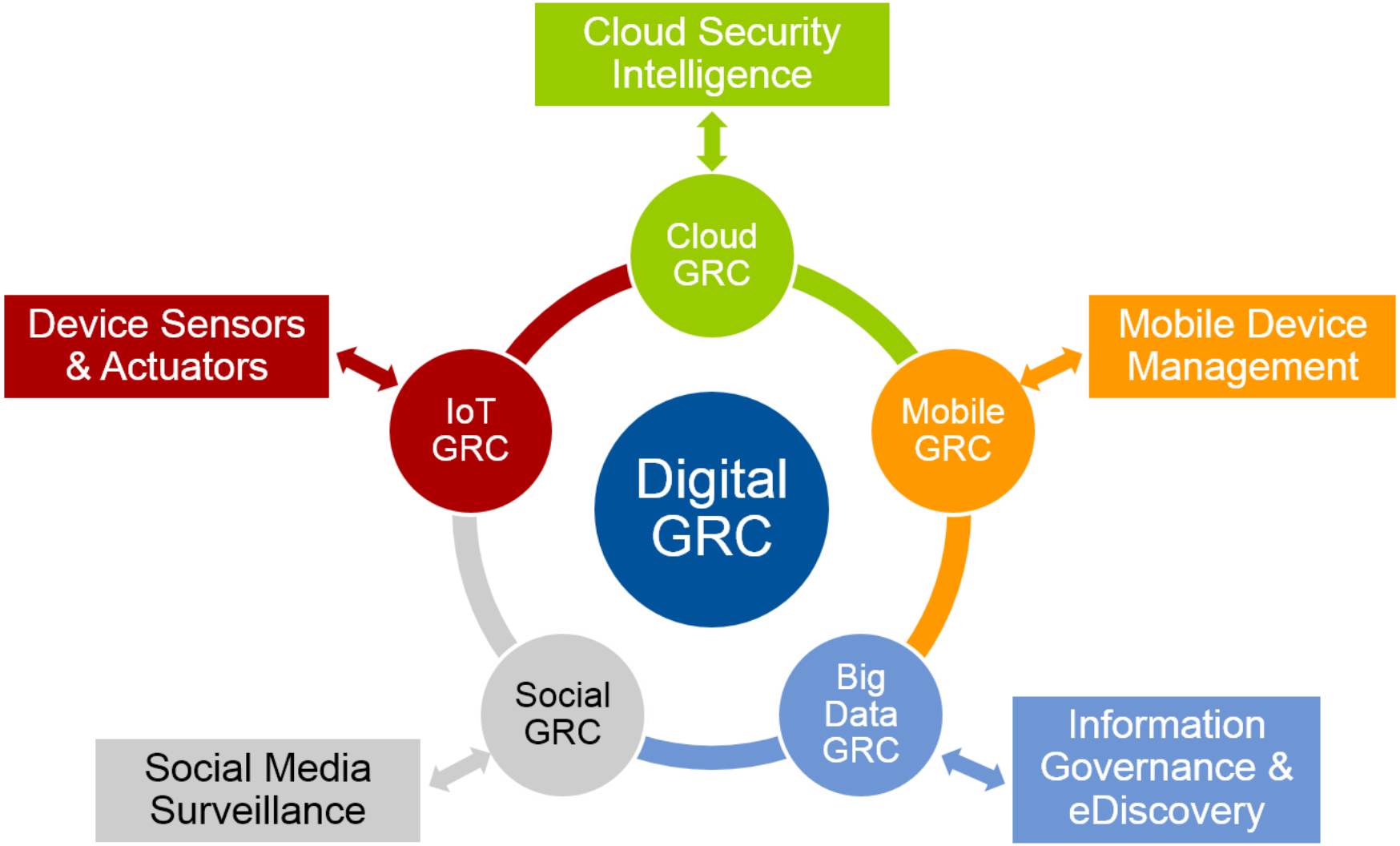
ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada.

GRC

- Gobierno, Riesgo y Cumplimiento.

- Término sombrilla, cada vez más utilizado que cubre estas tres áreas de actividades de las empresas.

- Estas áreas de actividad están siendo progresivamente más alineados e integrados para mejorar el rendimiento de la empresa y la entrega de las necesidades de las partes interesadas.


Cloud Security Intelligence
Cloud GRC
Device Sensors & Actuators
IoT GRC
Digital GRC
Mobile GRC
Mobile Device Management
Social GRC
Big Data GRC
Social Media Surveillance
Information Governance & eDiscovery

Componentes para apoyar la Auditoría de TI

Definir las TI

- Áreas a tomar en cuenta y aspectos a considerar en el plan de Auditoría.

Evaluar los Riesgos

- Conciencia de la evolución del riesgo tecnológico y su valoración en función del negocio.

Definir el universo

- Establecer el alcance de la Auditoría de TI y definir los recursos acorde a los requerimientos del programa.

Ejecutar la Auditoría de TI

- Aplicación de los programas y procedimientos en el campo de trabajo.

Guía de Auditoría de Tecnología Global (GTAG-4)-IIA

6 pasos efectivos para una gestión de auditoria de TI.

1. Asegúrese de que la base de su auditoría no tiene ningún 'cracks'

2. Determinar el nivel de riesgo en las decisiones basándose en los sistemas de información

3. Preparar una respuesta que finaliza una estrategia para abordar las deficiencias

4. Asegúrese de que los recursos disponibles son suficientes

5. Finalizar un modelo para la realización de actividades de análisis de datos

se alcanzan 6. Controlar y mejorar las actividades para asegurar que los resultados deseados

Fuente:casewareanalytics.com

INFORMACIÓN DE CONTACTO

cdhilario@Gmail.com

Tel. 809-850-6892

¡Gracias por su Atención!

PREGUNTAS