



Estado Libre Asociado de Puerto Rico  
**OFICINA DEL CONTRALOR**

# **LA IMPORTANCIA DE LA AUDITORÍA DE SISTEMAS EN LA INTEGRIDAD DEL SERVICIO PÚBLICO Y PRIVADO**

Universidad del Sagrado Corazón

Manuel Díaz Saldaña  
9 de mayo de 2007

# Constitución del Estado Libre Asociado de Puerto Rico Art. III, Sec. 22

El Contralor fiscalizará todos los ingresos, cuentas y desembolsos del Estado, de sus agencias e instrumentalidades y de los municipios, para determinar si se han hecho de acuerdo con la ley. Rendirá informes anuales y todos aquellos informes especiales que le sean requeridos por la Asamblea Legislativa o el Gobernador.



# Estado Libre Asociado de Puerto Rico

## OFICINA DEL CONTRALOR

### MISIÓN

Fiscalizar y promover el uso efectivo y eficiente.

### VISIÓN

Ser modelo de administración pública y servir de agente de cambio para promover el uso honesto de los recursos.

### VALORES

Cinco, fundamentales para el logro de la misión y la visión.

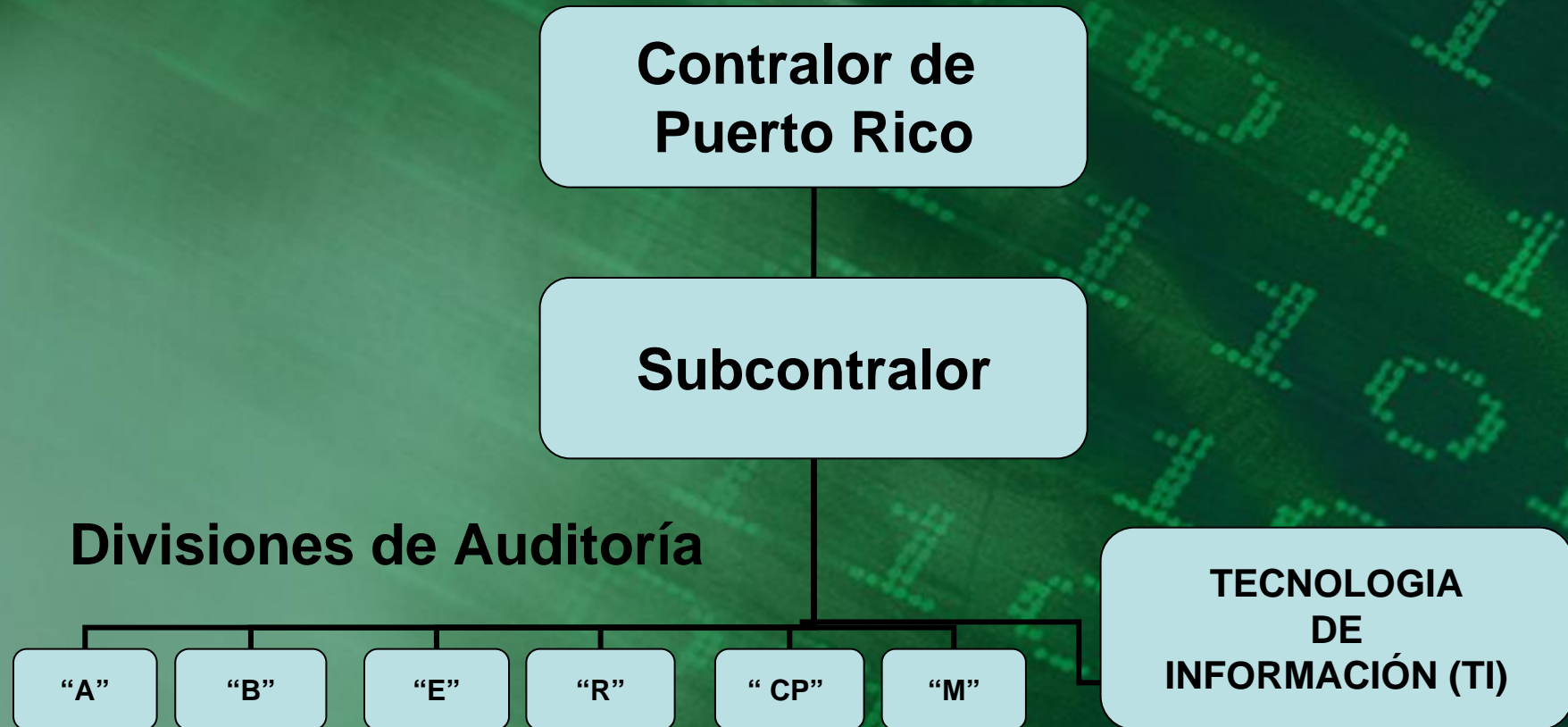


# Constitución del Estado Libre Asociado de Puerto Rico Art. VI, Sec. 9

Sólo se dispondrá de las propiedades y fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado, y en todo caso por autoridad de ley.



# Oficina del Contralor Área de fiscalización



# Posición del Auditor en la gobernanza



# Objetivos de una empresa

- Planificar (estratégicos)
- Ser efectivo y eficiente (operacionales)
- Cumplir con las leyes y los reglamentos (de cumplimiento)
- Contar con y proveer información financiera correcta, confiable (de informes)

**ESTRUCTURA INTEGRADA DE CONTROL INTERNO (COSO 2004) - OCHO COMPONENTES**



# Tecnología y el logro de los objetivos

- Aumenta la capacidad de almacenamiento y organización de la información
- Mejora la capacidad de análisis y evaluación de la información
- Amplía y mejora el acceso y la divulgación de la información
- Amplía y mejora las actividades de control (mediciones, estándares, indicadores, exactitud)



# Experiencia en Puerto Rico

Aumento significativo en el uso de tecnología de información

- ✓ Entidades con centros de sistemas de información

**1975**

**2007**

---

35

138

- ✓ Ley de Gobierno Electrónico (Ley Núm. 151 de 22 de junio de 2004, según enmendada)



# Riesgos inherentes

- Inversión de fondos vs vida útil de la tecnología vs resultados esperados
- Costos excedan los fondos comprometidos
- No se pueda garantizar la disponibilidad, confidencialidad y exactitud de la información generada y los datos conservados
- Tentación (uso inapropiado)
- Intromisión de externos (ataques)



# Leyes que atienden los riesgos

- Ley Núm. 96, 15 jul. 1988 según enm. – *Ley de Propiedad Intelectual*
- Ley Núm. 81, 30 ago. 1991 según enm. – *Ley de Municipios Autónomos del Estado Libre Asociado de Puerto Rico*
- Ley Núm. 259, 29 dic. 1995 según enm. – *Bonos, Sistemas de Informática Electrónica*
- Ley Núm. 220, 2 sept. 2003 según enm. – *Ley para Garantizar el Acceso de Información a las Personas con Impedimentos*



## Cont. Leyes que atienden ...

- Ley Núm. 151, 22 jun. 2004 según enm. - *Ley de Gobierno Electrónico*
- Ley Núm. 111, 7 sept. 2005 según enm. - *Ley de Información al Ciudadano sobre Seguridad de Bancos de Información*
- Ley Núm. 243, 10 nov. 2006 según enm. - *Ley para disponer la política pública sobre el uso del número de seguro social como verificación de identificación y la protección de su confidencialidad*



## Cont. Leyes que atienden ...

- *Health Insurance Portability and Accountability Act (HIPAA), 1996*
- *Financial Services Modernization Act (Gramm-Leach-Bliley Act – GLBA), 1999*
- *Ley Sarbanes Oxley, 2002*
- *Federal Information Security Management Act (FISMA), 2002*



# Exigencias relevantes

- a. Tomar acciones para eliminar o disminuir riesgos
- b. Auditorías que resulten en cero hallazgos
- c. Garantizar la integridad de los datos
- d. Manejo continuo de riesgos
- e. Garantizar la continuidad de los procesos críticos
- f. Mejorar la eficiencia operativa
- g. Detectar, reconciliar e informar incidentes (efecto material en las operaciones)
- h. Proteger los datos de carácter personal
- i. Proteger los activos de la entidad
- j. Prevenir o tomar medidas correctivas



# Mejores prácticas



- Las Mejores Prácticas para la adquisición, desarrollo, utilización y control de la tecnología de información



- Recomendaciones para combatir la corrupción y fomentar buenas prácticas de Administración Pública (Plan CTC 2004)



# Tres Pasos a Seguir

Establecer una cultura de rendición de cuentas y de valores éticos

Desarrollar una función óptima de auditoría interna

Cumplir con los estándares de la industria



## Cont. Tres Pasos a Seguir

1. Establecer una cultura de rendición de cuentas y de valores éticos

- Asignar recursos
- Emitir y divulgar códigos de ética internos
- Velar por cumplimiento de códigos de ética – internos, externos y de la profesión



## Cont. Tres Pasos a Seguir

### 2. Desarrollar una función óptima de auditoría interna

- identificar las fortalezas y las debilidades
- identificar y resolver los problemas
- dota a la institución de la agilidad necesaria para alcanzar la excelencia y optimizar sus procesos



## Cont. Tres Pasos a Seguir

Desarrollar una función óptima de auditoría interna - **TECNOLOGÍA DE INFORMACIÓN**

- Uso de tecnología para el manejo y control de cambios
- Uso de herramientas tecnológicas para:
  - Prevenir
  - Auditar
  - Identificar
  - Remediar (corregir)



# AUDITORÍA DE SISTEMAS



Hallazgos más  
frecuentes



# Hallazgos más frecuentes

- Uso de microcomputadoras y cuentas en asuntos ajenos a la función pública
  - acceder a la Internet
  - correo electrónico (envío y recibo de mensajes)
  - preparación de documentos
- Instalación de programas ajenos al interés público



## Cont. Hallazgos más frecuentes

- Fallas en parámetros de seguridad
  - No se establecen los niveles de acceso necesarios - solo el personal autorizado
  - Permiten a usuarios no autorizados o cuyas funciones no corresponde, alterar estándares de seguridad o información en las bases de datos
  - Uso de cuentas de acceso y contraseñas por períodos ilimitados
  - Falta de segregación de funciones



## Cont. Hallazgos más frecuentes

- Falta de controles
  - No tienen actualizadas las definiciones del programa de antivirus (*virus definitions*) - prevenir y detectar programas no deseados
  - No han instalado la pantalla de advertencia sobre el uso del equipo
  - No se requiere el uso de contraseñas para desactivar el protector de pantalla en las computadoras



## Cont. Hallazgos más frecuentes

- *Cont. Falta de controles*
  - No se requiere que las contraseñas contengan el mínimo de caracteres adecuado, ni la combinación de éstos
  - No se requiere el cambio de contraseñas periódicamente
  - No se define la cantidad de intentos de acceso sin éxito para deshabilitar la cuenta
  - No se define el tiempo de acceso de acuerdo a las funciones del usuario (*time restrictions*) o se tiene acceso excesivo



## Cont. Hallazgos más frecuentes

- *Cont. Falta de controles*
  - No se desactivan cuentas sin uso por períodos prolongados prestablecidos
  - Cuentas que nunca se han conectado permanecen activas
  - No se desactivó la cuenta de “invitado” (*Guest*)
  - No se activa la opción de políticas de auditoría (*Audit Policy*) que verifica diferentes eventos de control



## Cont. Hallazgos más frecuentes

- Falta de normas y de procedimientos escritos para:
  - la administración, la seguridad y el uso de los sistemas de información
  - la actualización de bases de datos – solicitud, autorización, realización, aprobación y verificación (responsabilidad y documentación)



## Cont. Hallazgos más frecuentes

- Ausencia de:
  - Informe de Avalúo de Riesgo
  - Plan de Seguridad
  - Plan de Continuidad de Negocios
  - Pruebas o simulacros
- Deficiencias en el Plan de Contingencias
- Ausencia de fiscalización



## Cont. Tres Pasos a Seguir

### 3. Cumplir con los estándares de la industria

- Estructura Integrada de Control Interno (emitida por el *Committee of Sponsoring Organizations – COSO – 1992*)
- *Control Objectives for Information and Related Technology (CobiT)* (emitido por la Asociación para la Auditoría y Control de Sistemas de Información – *ISACA - 1992*)
- Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (desarrolladas por empresas privadas)



# RECOMENDACIONES DE LA OFICINA DEL CONTRALOR

## Estrategias para Mejorar la Administración Pública



- Fiscalización rigurosa y constante
- Promover la educación y el adiestramiento
- Promover un sistema administrativo y financiero de excelencia con énfasis en los controles internos efectivos
- Leyes justas
- Castigos disuasivos
- Alianzas estratégicas



***No podemos resolver los  
problemas utilizando el  
mismo nivel de pensamiento  
que usamos para crearlos.***

***Albert Einstein***



# ¿Preguntas?



*Contraloría a sus órdenes...*

# Contacto con la OCPR



**Alina E. Torres Marrero**

Contralor Auxiliar/Anticorrupción

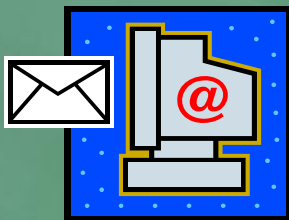
787-250-3316

787-754-3030 ext. 2750



PO Box 366069

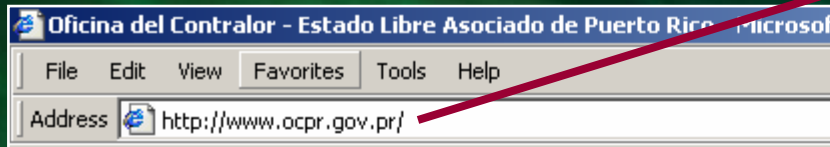
San Juan, PR 00936-6069



[atorres@ocpr.gov.pr](mailto:atorres@ocpr.gov.pr)



*Contraloría a sus órdenes...*



[www.ocpr.gov.pr](http://www.ocpr.gov.pr)

SISTEMA DE BÚSQUEDA

E-mail  
[ocpr@ocpr.gov.pr](mailto:ocpr@ocpr.gov.pr)



Contraloría a sus órdenes...

