



**IX JORNADA
de SEGURIDAD
INFORMATICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Reflexiones sobre IT-GRC

Preparado por:

Astrid Pereira Sierra

Astrid@creangel.com





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Agenda

- Conceptos
- GRC
- IT-GRC



IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Metas

- Reconocer
- Prevenir
- Controlar
- Mejorar conducta corporativa
- Proteger reputación (visto como Basilea)
- Consistencia con objetivos estratégicos
- Generar confianza
- Mejorar competitividad
- Determinar estado real
- Prevenir Fraudes
- Prevenir Incumplimientos



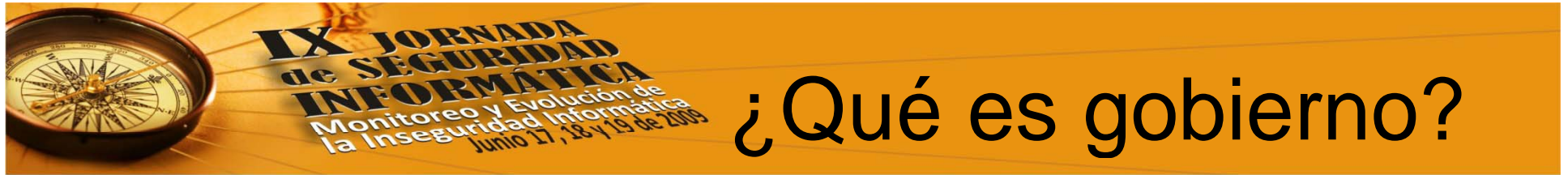


**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Para comenzar...

- Las empresas existen para ofrecer valor a sus interesados (Accionistas, trabajadores, país etc.) generando valor, asumiendo riesgos y usando los recursos disponibles de una forma responsable para alcanzar las metas fijadas.
- Las decisiones deben ser tomadas rápidamente, el seguimiento se comparte entre muchas personas por lo cual una buena estrategia de gobierno facilita el logro de metas con transparencia.





- Es el marco de trabajo, principios, estructura, procesos y practicas para establecer directivas, verificar su cumplimiento con el fin permanecer alineado con el propósito, estrategia y objetivos de la empresa



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

Gobierno

Tiene que ver con la responsabilidad de buscar transparencia, mediante la definición de mecanismos utilizados para el seguimiento de los procesos y políticas de tal forma que una vez establecidos se cumplan con el fin de tomar medidas y acciones correctivas cuando las reglas no se siguen o sean susceptibles de mejora





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Risk Management



- Riesgo es la contingencia de un daño
- RM es un proceso mediante el cual el riesgo se identifica, prioriza, mitiga, acepta o transfiere basado en los objetivos de la organización.



**IX JORNADA
de SEGURIDAD
de INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

Sobre el riesgo...

- Asumir una cierta cantidad de riesgo es prácticamente inevitable para las organizaciones en la búsqueda de alcanzar sus objetivos. La administración de riesgo ayuda a administrar proyectos y a mejorar el rendimiento operativo permitiendo:
 - Ofrecer certezas y minimizar “sorpresas”
 - Mejorar la calidad de servicio ofrecido
 - Mejorar la administración de cambios
 - Uso más eficiente de recursos
 - Mejorar en el proceso de toma de decisiones
 - Reducción del desperdicio
 - Administración de contingencias





IX JORNADA de SEGURIDAD INFORMÁTICA

Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009



RISK ASSESSMENT

It's Not Worth It

DIY.DESPARL.COM





Cumplimiento

- En general cumplimiento significa obrar de manera acorde a una especificación, política, estándar o ley claramente definido
- Se convierte en un proceso que registra y monitorea los controles necesarios para alinearse con los mandatos (internos o externos) aplicables a la organización





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

IT-GRC

FORRESTER®

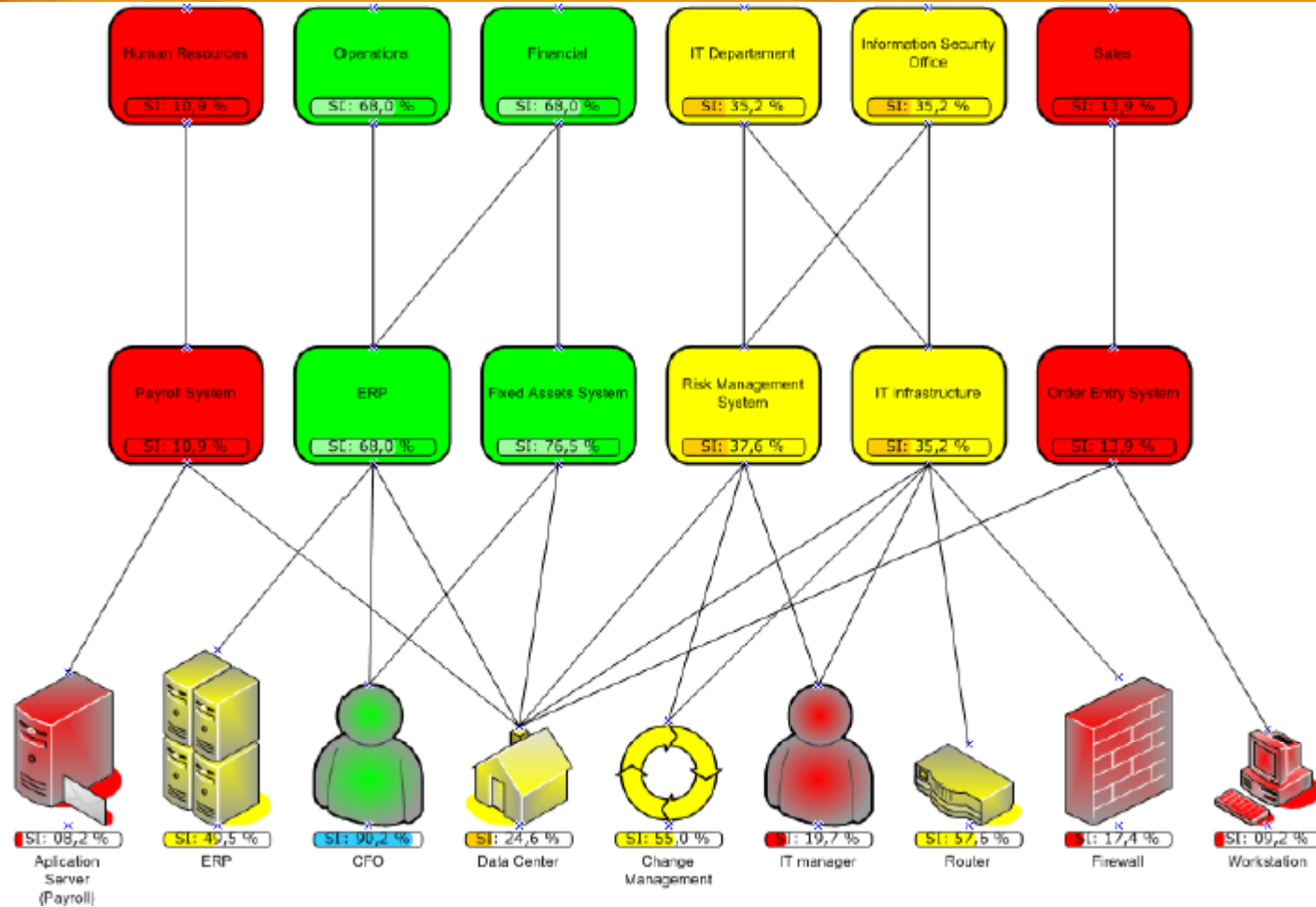
- Gobierno de IT, Administración de riesgo de IT (IT-GRC por sus siglas en inglés) y cumplimiento de IT son disciplinas diferentes que en el pasado existían como islas que manejaban proyectos de ejecución única en porciones pequeñas de la organización.
- IT-GRC identifica elementos comunes y relacionados entre áreas permite una aproximación que crea eficiencias, provee una visión holística de IT, asegura responsabilidades, mejora la efectividad y permite mejoras en seguridad de la información





IX JORNADA de SEGURIDAD de INFORMATICA

Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009



Fuente: Modulo IT GRC



**IX JORNADA
de SEGURIDAD
INFORMATICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Habilitadores de IT GRC

- Políticas mandatorias
- Presión regulatoria
- Requerimientos de clientes





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

Gobierno de IT

Facilita:

1) Establecer estructuras de decisión y mecanismos de seguimiento

- Quien decide, cómo decide, quien responde, como se miden y monitorean resultados
- La organización debería tener estructuras de gobierno como comités de tecnología, de arquitectura y revisores de proyectos



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Gobierno de IT (2)

- 2) Asegurar que existen procesos apropiados para garantizar consistencia y transparencia Ej. Procesos para proponer nuevos proyectos, aprobación de inversiones en IT y priorización de proyectos de IT



Gobierno de IT (3)

3) Asegurar que hay una comunicación apropiada, monitoreo y responsabilidad para medir las decisiones de IT dado que estas involucran elementos técnicos, humanos, avance de proyectos, análisis de retorno entre otros



Administración de riesgo de TI

Ayuda a:

- **Mitigar efectos adversos e identificar oportunidades**
 - Los ambientes tecnológicos son mas complejos y la dependencia de TI es mayor. Los directores de TI y los oficiales de seguridad deben manejar diferentes tipos de amenazas mientras ofrecen mayor valor al negocio lo cual implica adaptarse a los cambios en las necesidades del negocio y prever adversidades.
 - La arquitectura tecnológica debe ofrecer flexibilidad y eficiencia



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Cumplimiento en TI

Debería permitir asegurar que la organización:

- Se adhiere a la ley y las regulaciones
- Considera responsabilidades y se apega a estándares
- Respeto la propiedad intelectual
- Utiliza marcos de control basados en estándares

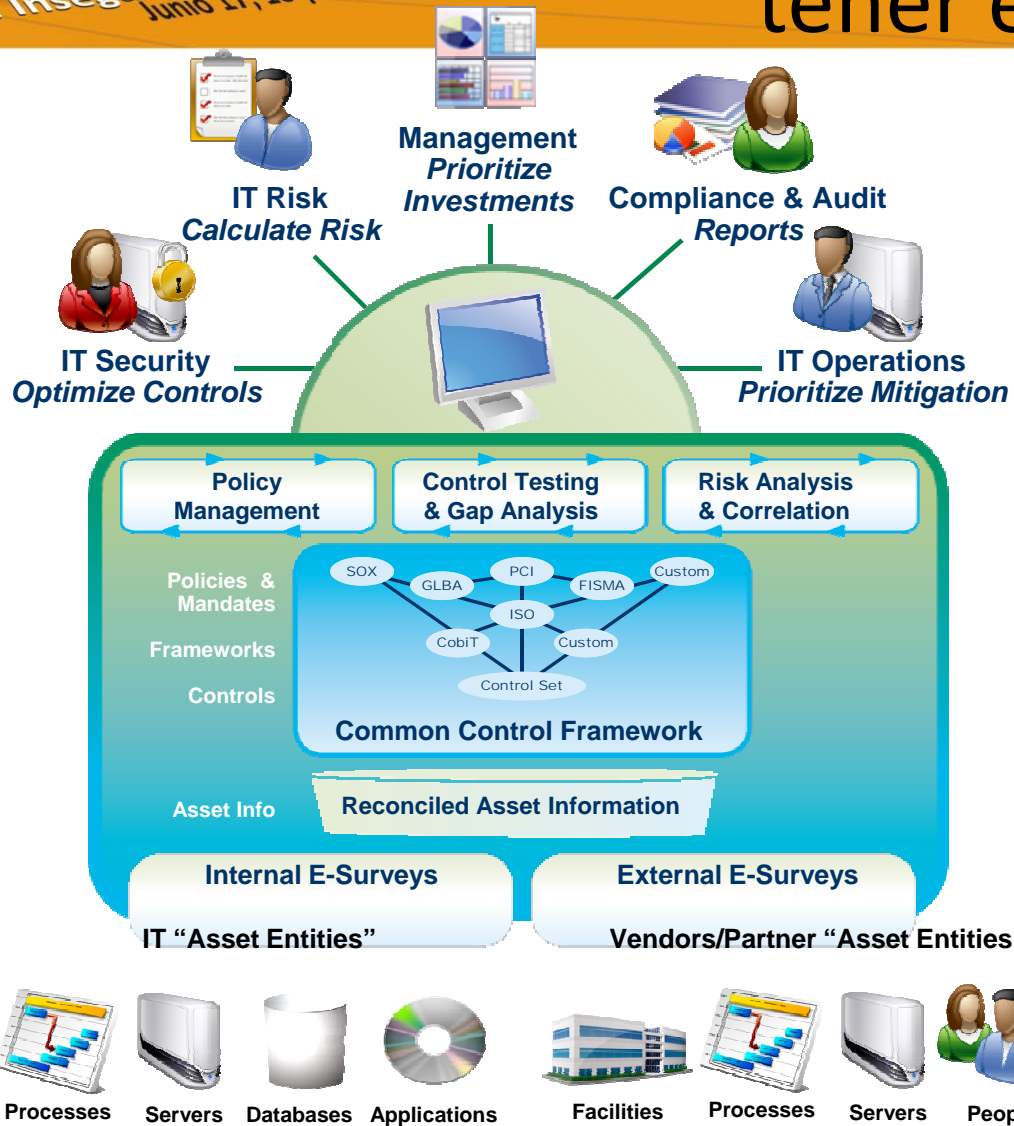


Las actividades de cumplimiento incluyen:

- Conducir investigación sobre regulaciones
- Diseño de controles de TI
- Aconsejar a TI o a terceros respecto a los requerimientos de control
- Revisar y reportar los avances en cumplimiento con elementos mandatorios y regulaciones



Elementos a tener en cuenta



Fuente: Agilience





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Efectividad en IT GRC

Entienda las dependencias y busque elementos comunes

- G,R y C dependen uno del otro
 - Las medidas de gobierno usan marcos de control y cumplen con requerimientos que ayudan a definir estrategias en TI. El cumplimiento se apoya en TI y los riesgos identificados para alcanzar metas y la administración de riesgo toma como base actividades de gobierno y medidas de cumplimiento para determinar el riesgo existente. Tener clara la sinergia y coordinarla mejoran la efectividad



Unifique controles para administración de riesgo y cumplimiento en TI

- El proceso para identificar y reportar riesgo y cumplimiento en TI pueden ser diferentes pero es posible apoyarse en frameworks para establecer y medir controles de seguridad
- Los frameworks a usar deberían satisfacer requerimientos de cumplimiento internos y externos para evitar duplicación de esfuerzos, asegurar consistencia y evitar islas
- El factor crítico de decisión de la herramienta es que tanto puede automatizar la recolección de información



**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

Facilite el gobierno estableciendo responsabilidades

Establecer responsabilidades es clave en IT GRC

- Establezca responsabilidades:

- Asegure que

- Roles
- Estructuras de gobierno
- Procesos

Estén CLARAMENTE articulados, comunicados y comprendidos por sus directivos, empleados e interesados

- Asegure también que:

- Hay mecanismos de medida y reporte de áreas críticas y reajuste el plan basado en estas medidas



Estándares y frameworks alrededor de GRC



HIPAA

SOX

GLBA

COSO

FFIEC

Basel II

DOD 8500.1 & 8500.2

DISA STIGS

CobiT

FISMA

NERC

ISO 31000

PCI

ISO 27005

NIST SP800

DCID 6.3

OMB 06-16, OMB 07-16, and HSPD-12

SB 1386

ISO 17799/27001/27002

PCI DSS

DIACAP





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

Alinee la tecnología los procesos para la eficiencia y la consistencia

- La tecnología juega un rol importante en la automatización, acumulación, análisis y reporte de controles de tecnología NO es el único componente necesario para establecer y definir puntos de unión de actividades entre IT g,r y c primero establezca el conjunto de procesos y luego use tecnología para automatizar



IX JORNADA de SEGURIDAD de INFORMÁTICA
 Monitoreo y Evolución de la Inseguridad Informática
 Junio 17, 18 y 19 de 2009

Ciclo de IT-GRC



Scope Assets

Intelligent Profiling

- People
- Processes
- IT Infrastructure
- Applications
- Buildings
- Partners
- Vendors
- Objectives
- Organizations



Select

Common Control Framework

- Regulations and Mandates
- Standard Frameworks
- Controls and Subcontrols
- KRIs** (Key Risk Indicators)
- ERM** Collaboration



Run

Control Test Automation

- Human Attestation
- eSurveys
- Technical Control Tests
- Security Mgmt. Integration
- Risk & Compliance Scoring



Decide

Risk-based Prioritization

- Risk Rationalized Tickets
- ALE & ROI Analysis
- Mitigation ROI Optimizer
- Ticket Closure Workflow



Act

Consolidated View

- Risk & Compliance Process Management
- Role-Based Dashboards
- Trending
- Custom Reports
- Report Templates:
 - Compliance
 - Risk Assessment s
 - Entity (Asset)
 - Ticket Analysis
 - Surveys
 - ERM Summaries



Fuente: Agilience





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
La Inseguridad Informática
Junio 17, 18 y 19 de 2009

Mas allá de IT-GRC

- El alcance de GRC va mucho mas allá de tecnología (IT).
- Sin embargo el más complejo es IT-GRC (por la automatización)
- Es importante tener en cuenta a los terceros (Vendor) que acceden a la infraestructura.
- No sólo existe luego de consolidar IT-GRC y Vendor GRC, se considera un paso natural Project GRC.





GRC algunas consideraciones

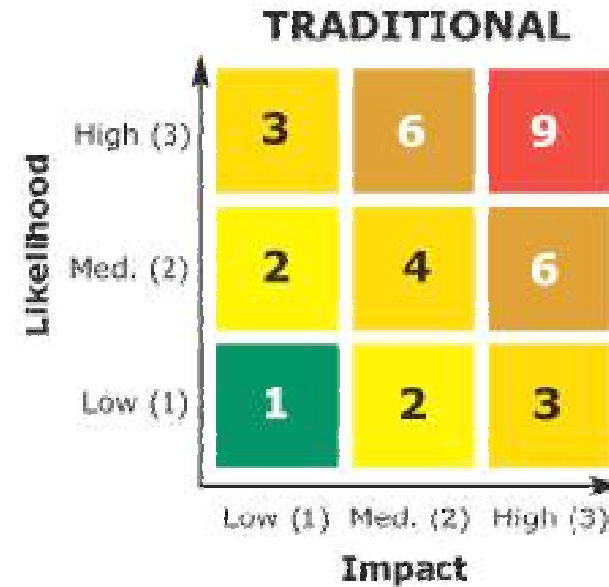
- Expanda la visión mas allá de IT
- Con el tiempo Incluya elementos tales como riesgo operacional (ORM por sus siglas en ingles)
- Riesgo financiero
- Establezca un indicador de riesgos claves (KRI por sus siglas en ingles)
- Genere un indicador de riesgo empresarial (ERM por sus siglas en ingles)
- Esto le dará la verdadera convergencia y visión holística que tanto piden las gerencias y juntas directivas



**IX JORNADA
de SEGURIDAD
INFORMATICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

implementación de GRC

- IT-GRC -> Vendor GRC -> Project GRC
- IT-GRC -> ORM -> ERM
- ERM -> KRI





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Automatización de GRC

- Busque soluciones que se integren con lo que ya tiene
- Si su empresa es grande no intente llevar todo en hojas de calculo (no va a tener resultados consistentes)
- Trate de hacer repetible el proceso en el tiempo
- Un paquete no es la solución mágica necesita gente que lo apoye
- Busque paquetes que le permitan tener segregación de funciones
- Modelar su empresa es la clave (que se ajuste el paquete a su organización y no al revés)





Fallas comunes en IT GRC y GRC

- Pensar que GRC es solo tecnología
- No definir claramente las responsabilidades
- Posponer el componente tecnológico
- No abordar los controles desde un modelo de integración
- No reconocer el valor de IT GRC para la organización



PREGUNTAS?

- GRACIAS!