CIBERSEGURIDAD - UNA VISIÓN ESTRATÉGICA.

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Incidentes referidos a TI - Internacionales

02/2018

Filtración de datos de seguridad

03/2018

Facebook

GDPR

Indagación

Reacción

04/2018

1.5 millones de registros expuestos en Amazon S3 (Panamá papers)

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Incidentes referidos a TI - Internacionales

.

04/2018

.

Australia: 1.5 millones de detalles de clientes potencialmente robados.

Atacaron el sistema de pagos electrónicos.

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

¿TU ESTRATEGIA DE SEGURIDAD ES LA MISMA DE HACE 10 AÑOS?

Las amenazas vienen avanzando en estos últimos

10 años…

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

TWITTER INOFENSIVO?????

https://www.bleepingcomputer.com/news/security/russian-state-hackers-use-britney-spears-instagram-posts-to-control-malware/

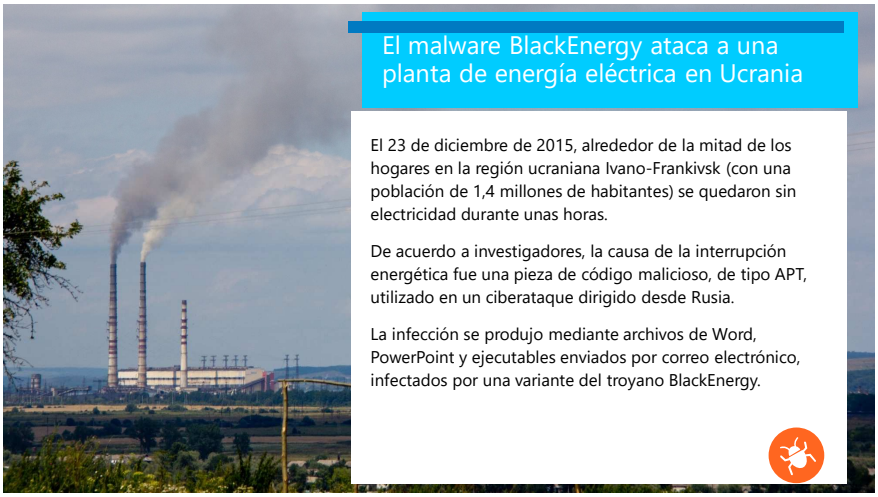
Si miramos de cerca al link

http://bit.ly/**2kdhuHX**

bit.ly URL:

smith2155< 200d >#2hot ma< 200d >ke lovei< 200d >d to < 200d >her, < 200d >uupss < 200d >#Hot < 200d >#X

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.



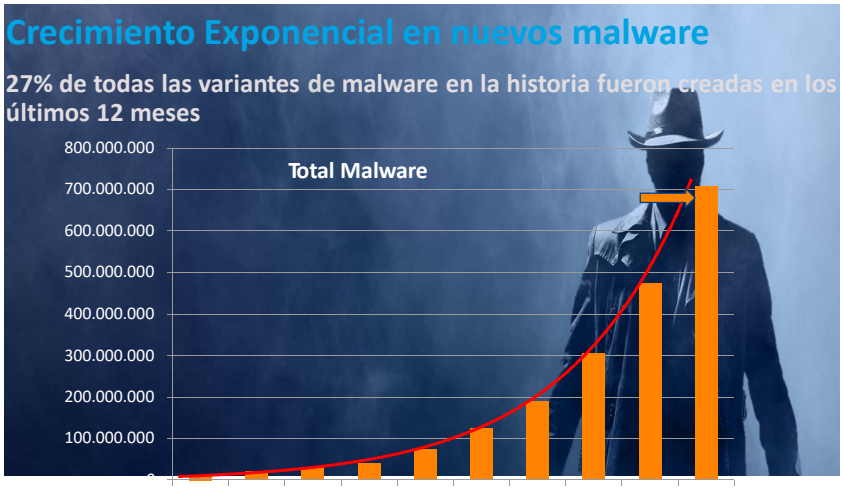
El malware BlackEnergy ataca a una planta de energía eléctrica en Ucrania

El 23 de diciembre de 2015, alrededor de la mitad de los hogares en la región ucraniana Ivano-Frankivsk (con una población de 1,4 millones de habitantes) se quedaron sin electricidad durante unas horas.

De acuerdo a investigadores, la causa de la interrupción energética fue una pieza de código malicioso, de tipo APT, utilizado en un ciberataque dirigido desde Rusia.

La infección se produjo mediante archivos de Word, PowerPoint y ejecutables enviados por correo electrónico, infectados por una variante del troyano BlackEnergy.

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.



Fuente: AV-TEST

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Incidentes referidos a TI - Locales

2012 2014 2016 2018

08/2012

02/2015

28/03/2018

02/2012; 01/2014; 02/2018

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Actitud de las partes interesadas.

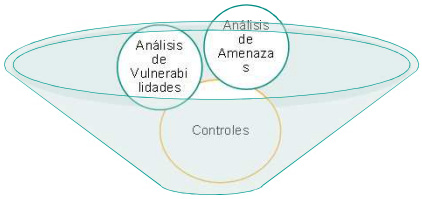
CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Y por casa; cómo estamos?

?

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Foco en GRC

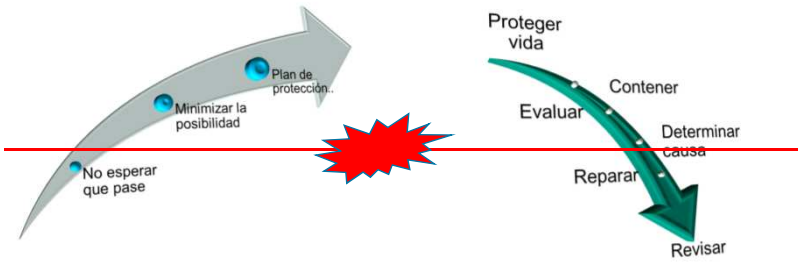


Estrategia

Fuente: ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

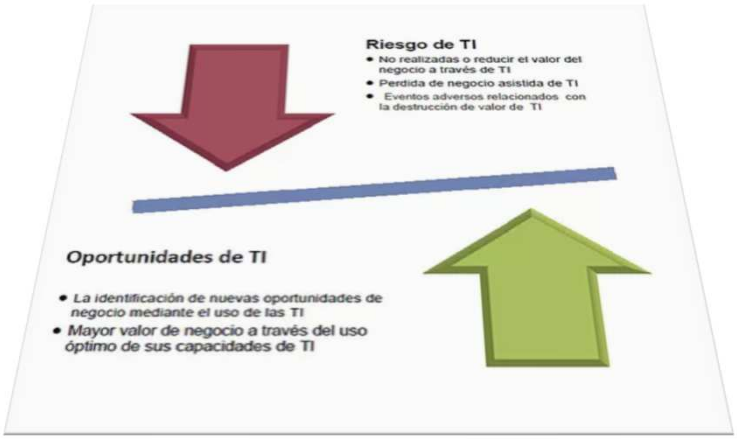
Foco en GRC



Fuente: Microsoft

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Foco en GRC



Fuente: ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Foco en GRC

Fuente: ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

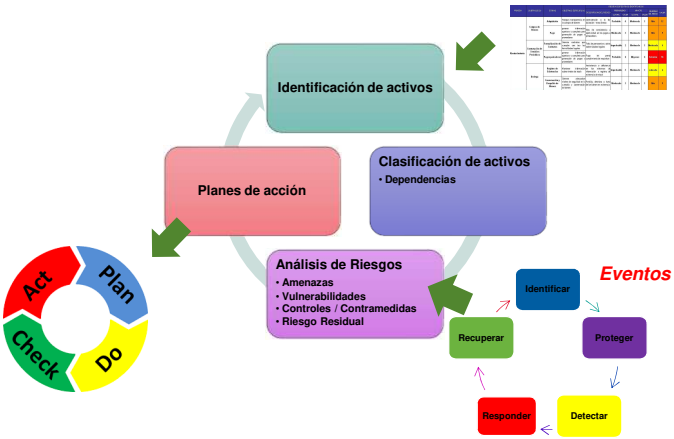
Foco en GRC

Jerarquía de Riesgos de TI

Fuente: ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI



Fuente: ISO 27001 · NIST National Institute of Standards and Technology U.S. Department of Commerce · ISO 22301:2012

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI; Identificación de activos

PROCESO	SUBPROCESO	ETAPAS	OBJETIVOS ESPECIFICOS	DESCRIPCION DEL RIESGO	PROBABILIDAD		IMPACTO		SEVERIDAD DEL RIESGO	VALOR
					CLASIFIC.	VALOR	CLASIFIC.	VALOR		
	Compra de Bienes	Adquisición	Asegura transparencia en la compra de bienes	contravención a la ley licitación - trata directo	Probable	4	Moderada	3	Alto	12
		Pago	generar información oportuna y completa para la generación de pagos a proveedores	falta de consistencia u oportunidad en los pagos a proveedores	Moderado	3	Moderado	3	Alto	9
	Contratación de Servicios Periodicos	Formalización de Contratos	Generar contratos que cumplan con tos las formalidades legales	Falta de personerias u otras solemnidades legales	Improbable	2	Moderado	3	Moderado	6
		Pagos periodocos	generar información oportuna y completa para la generación de pagos a proveedores	Pago sin previo cumplimiento de requisitos	Probable	4	Mayores	4	Extremo	16
stecimiento	Bodega	Registro de Existencias	Mantener información sobre niveles de stock	inexistencia o deficiencia en los sistemas de información y registro de existencia de stock	Improbable	2	Moderado	3	oderado	6
		Conservación y Respaldo de Bienes	Generar adecuados niveles de seguridad en la custodia y conservación	Perdida, deterioro o hurto de los bienes en existencia	Moderado	3	Moderado	3	Alto	9

Fuente: ISO 22301:2012

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

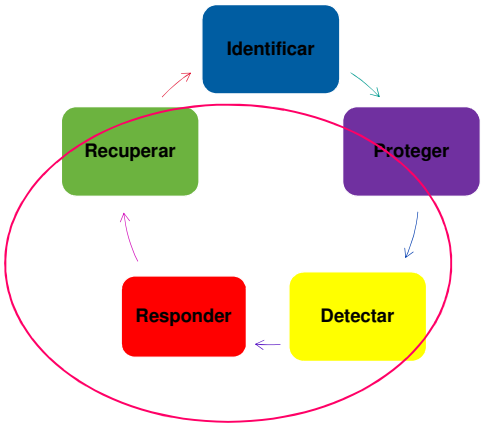
Proceso de GRTI;
Plan de acción

Fuente: ISO 27001

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI;
Eventos

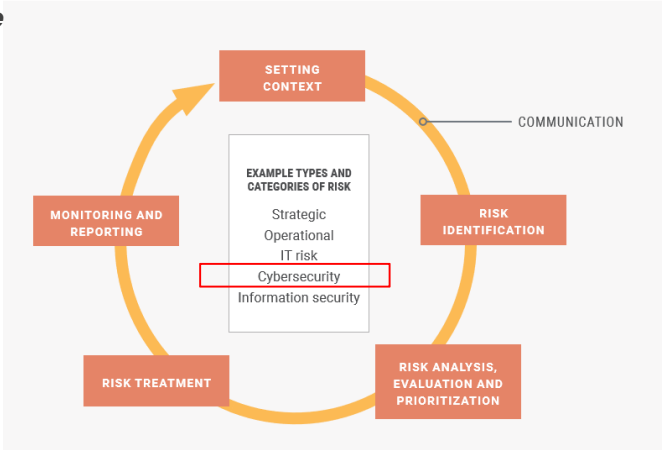


Fuente: NIST National Institute of Standards and Technology U.S. Department of Commerce

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

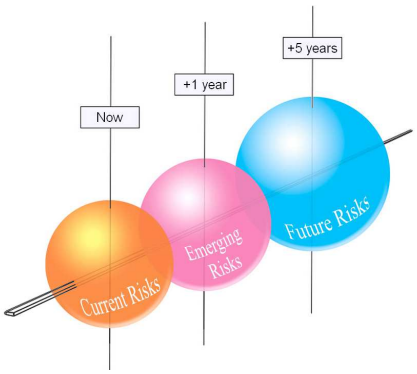
Proceso de GRTI; Alcance



Fuente: ISACA Getting Started with Risk Management - 2018

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI; Amenazas



Fuente: enisa

European Union Agency for Network and Information Security

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI;
Amenazas

La ventana de AREM (Amenazas y Riesgos empresariales).

Conocidos	Latentes	Focales	Emergentes
Malware	Ciberterrorismo	Ataques a sistemas de control industrial	Rootkits en PLC (controladores Lógicos programables)
Fuga de información	Ataques de día cero	Phishing dirigido	Malware en sistemas de control industrial
Botnets	Ciberespionaje	Vulnerabilidades en IoT	Computación en la niebla (Fog Computing)
Amenazas persistentes avanzadas	Ransomware (IoT, Móviles)	Ataques coordinados	USBDriveby

Fuente: ISACA La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial

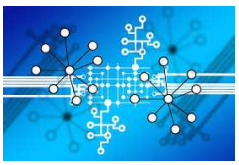
ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI (local)
Amenazas

BCRA – Com. A 4609 Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

BCRA – Com. A 4904. Régimen Informativo para Supervisión Trimestral / Anual (R.I. - S.) - "Base de datos sobre eventos de Riesgo Operacional".



Fuente: ISACA La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI (local)
Amenazas

BCRA – Com. A 5374-6017 Sección 6. Canales Electrónicos

Escenarios (19)

ECM001 Generación, distribución y descarte de credenciales que incluyen TC/TD.
ECM003 Suscripción, presentación, uso, renovación y baja de credenciales que incluyen TD/TC.
EDA001
Diseño, funcionalidad y homologación de dispositivos suministrados por la entidad o el operador.
…

Controles (94) referidos a:

Concientización y Capacitación;
Control de Acceso;
Integridad y Registro;
Monitoreo y Control y;
Gestión de Incidentes.

Fuente:

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI (local)
Amenazas

BCRA – Com. A 6354 *del 03/11/2017* Sec. 2. Desc. y tercerización de actividades.

Escenarios (4)

ESD001 *Datos del cliente. uso/explotación, conservación y transporte, incluyendo transacciones financieras que incluyan datos del cliente.*
ESD002 *Datos contables-financieros: uso/explotación, conservación y transporte, incluyendo o no datos de clientes.*
ESD003 *Datos transaccionales financieros: uso/explotación, conservación y transporte que no incluya datos del cliente.*
ESD004 *Datos operativos: uso/explotación, conservación y transporte que no incluya información contable-financiera, del cliente o transaccional financiera.*

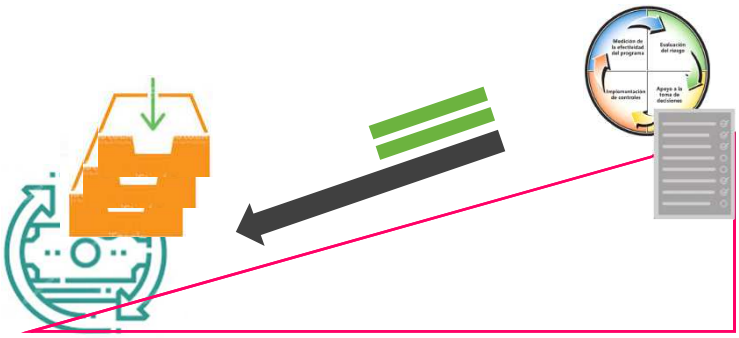
Controles (46) referidos a:

De Gobierno de seguridad de la información;
De Concientización y Capacitación;
De Control de Acceso;
De Integridad y Registro;
De Monitoreo y Control
De Gestión de Incidentes; y
Tabla de requisitos mínimos de Continuidad Operativa (PCN).

Fuente:

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI

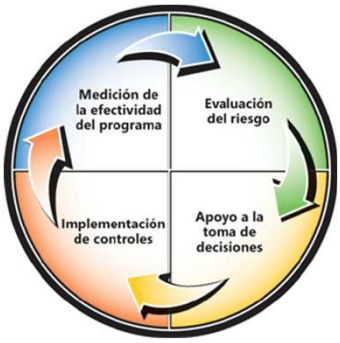


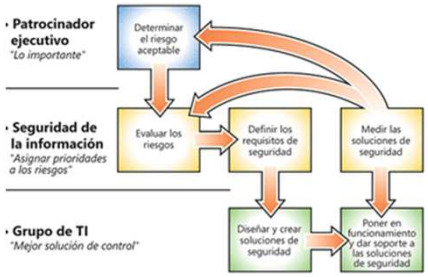
Fuentes: Magerit Microsoft

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI; Responsabilidades



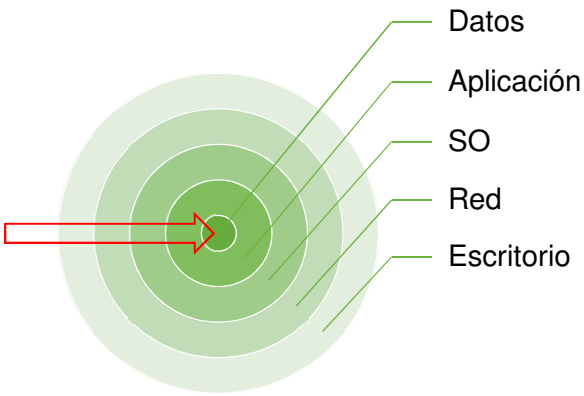


Fuente: Microsoft

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI;
Amenazas



Fuente: ISACA CISM Certified Information Security Manager

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI;
Amenazas

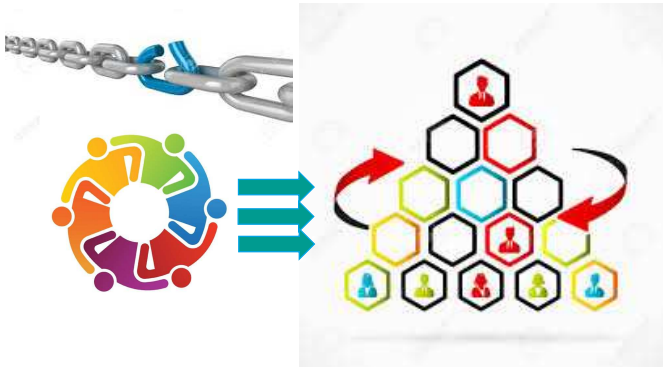
Fuente

OWASP (Open Web Application Security Project) .

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Proceso de GRTI;
Capacitación y concientización

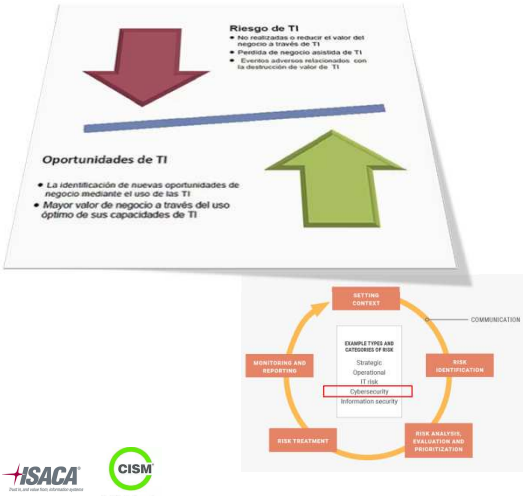


Fuente: ISACA — CISM Certified Information Security Manager

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Conclusiones



Fuente: ISACA — CISM Certified Information Security Manager

Se habla de estrategias de Ciberseguridad; pero cuántos análisis de riesgos contemplan estos escenarios???

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Conclusiones
Desafíos

Los incidentes **no son exclusivos de Seguridad de la Información** (Muchas veces la gestión de la seguridad queda en mano **de personas muy talentosas**).

Siempre qué hay un incidente de seguridad y deriva en una crisis **señalan al CIO y CISO**.

El desafío es el involucramiento de la dirección.

Realizar prácticas básicas en análisis de vulnerabilidades. Los ataques son masivos, más complejos y persistentes (combinados con ingeniería social). Se registran incidentes graves; temas de Machine Learning y Big Data conectados. Se presentan incidentes globales; que tienen reproducción; guerra Ciberseguridad entre países, ataques masivos, ataques más complejos y persistentes (combinados con ingeniería social)

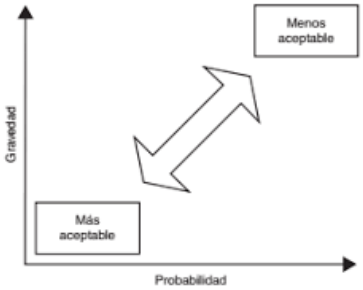
CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Conclusiones
Desafíos

- **Ser más proactivo y estar más preparado en la resiliencia.**
- ***Cada cambio es una nueva fuente de amenaza***.
- ***El intercambio de conocimientos y la comunicación*** ayudan a mitigar el riesgo.
- ***Tener plan estrategia y programa manejo de incidentes.***
- Considerar las amenazas dinámicas (distintas de las tradicionales).
- Monitoreo y detección temprana.
- Análisis de riesgos, determinar el alcance y escenarios; y documentar para **capacitar a todos los niveles.**
- ***¿Cómo concientizar sin pasar por un evento?.***

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Conclusiones



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

CSX CYBERSECURITY NEXUS

CISM Certified Information Security Manager® — An ISACA® Certification

Fuente: ISACA

Enfoque holístico de Evaluación de Riesgos de TI

ADACSI ISACA

CIBERSEGURIDAD; UNA VISIÓN ESTRATÉGICA.

Marcos de referencia

Microsoft

NIST National Institute of Standards and Technology U.S. Department of Commerce

Magerit

ITIL

ISO 20000

ISO 22301:2012

ISO 27001

ISACA

COBIT 5 AN ISACA® FRAMEWORK

CISA Certified Information Systems Auditor®

CRISC Certified in Risk and Information Systems Control™

CISM Certified Information Security Manager®

CSX CYBERSECURITY NEXUS

ADACSI ISACA

MUCHAS GRACIAS!!!!

Ing. Germán Gustavo Bollmann
CISM / LA LI ISO/IEC 27001 / LA ISO/IEC 22.301

ISACA Buenos Aires Chapter Leader.
Docente en UCA;
Profesional en Seguridad y Criptografía , Auditoría de Sistemas de Información
ggbollmann@Gmail.com
Linkedin: German.Bollmann Skype: ggbollmann Twitter: @ggbollmann

Héctor Calderazzi
CISA, CISM, CRISC, ITIL v3 Fundation y Auditor Líder ISO 9001.

ISACA Buenos Aires Chapter Leader.
Profesor en UCASAL; ISACA Bs As y Fundación Libertad Rosario.
Experto/Consultor en Gobierno de TI, Gestión de Riegos, Seguridad y Auditoría de Sistemas
hcalderazzi@gmail.com;
Linkedin: Héctor Calderazzi; Skype: hcalderazzi; Twitter: @hcalderazzi