
GOBIERNO DE SEGURIDAD, TECNOLOGÍA E INFORMACIÓN EN EL NEGOCIO
Gobierno y economía de la seguridad de la Información
ENTENDIENDO LA SEGURIDAD PARA LA TOMA DE DECISIONES
Septiembre 2021
API | Aseguramiento de Procesos Informáticos
RAS | Risk Advisory Services | IT Assurance, Audit and Compliance
BDO

1


LEADERS IN OUR MARKETS
CONEXIÓN GLOBAL. COMPRENSIÓN LOCAL.
BDO EN EL MUNDO
BDO EN ARGENTINA
RANKING
Puesto en el Ranking de auditoría global
5°
Puesto en el Ranking de auditoría local
OFICINAS
167 Países
+1.600
5
BUENOS AIRES
Retiro
Distrito Tecnológico
CÓRDOBA
MENDOZA
SANTA FÉ
Rosario
SOCIOS Y STAFF
+80.000
en el mundo
+600
en Argentina
BDO
API | Aseguramiento de Procesos Informáticos
RAS | Risk Advisory Services | IT Assurance, Audit and Compliance
AUDITORÍA Y CONTROL IT
CIBERSEGURIDAD Y FORENSIA DIGITAL
GOBIERNO DE TECNOLOGÍA E INFORMACIÓN
NORMATIVA Y EDUCACIÓN
GOVERNANCE, RISK & COMPLIANCE IT
DESARROLLO DE PROYECTOS ESPECIALES

2

API | Aseguramiento de Procesos Informáticos

RAS | Risk Advisory Services | IT Assurance, Audit and Compliance

Fabián Descalzo – Director (fdescalzo@bdoargentina.com)

Director y DPO de BDO en Argentina, a cargo del Departamento de Aseguramiento de Procesos Informáticos (API). Posee 30 años de experiencia en el área de gestión e implementación de Gobierno de Seguridad de la Información, Gobierno de TI, Compliance y Auditoría de TI en Argentina y Latinoamérica, y asesoramiento para el cumplimiento de Leyes y Normativas Nacionales e Internacionales en compañías de primer nivel de diferentes áreas de negocio. Docente del Diplomado Universitario en Accounting Tech en la Universidad Argentina de la Empresa - UADE del módulo BIG DATA Y SERVICIOS EN LA NUBE, Docente del módulo 27001 de las Diplomaturas de "IT Governance, Uso eficiente de Frameworks" y "Gobierno y Gestión de Servicios de TI" del Instituto Tecnológico Buenos Aires (ITBA), Docente del Módulo de Auditoría de IT de la Diplomatura en Delitos Informáticos para EDI en la Universidad Nacional de Río Negro y Docente en Sistemas de Gestión IT, Seguridad de la Información y Auditoría IT para TÜV Rheinland. Miembro del Comité Directivo de ISACA Buenos Aires Chapter, Miembro del Comité Directivo del "Cyber Security for Critical Assets LATAM" para Qatalys Global sección Infraestructura Crítica, Miembro del Comité Científico del IEEE (Institute of Electrical and Electronics Engineers)

ÁREAS DE CONOCIMIENTO

Riesgo, Gobierno y Auditoría de TI, Continuidad de Negocio y Recuperación de Procesos de Servicios de TI, Seguridad de la Información, Cumplimiento de Marco Regulatorio (SOX, HIPAA, PCI-DSS, Data Privacy, Internal Frame), Gobierno de Seguridad de la Información, Procesos de Servicios TI, Ciberseguridad

ESPECIALIZACIONES:

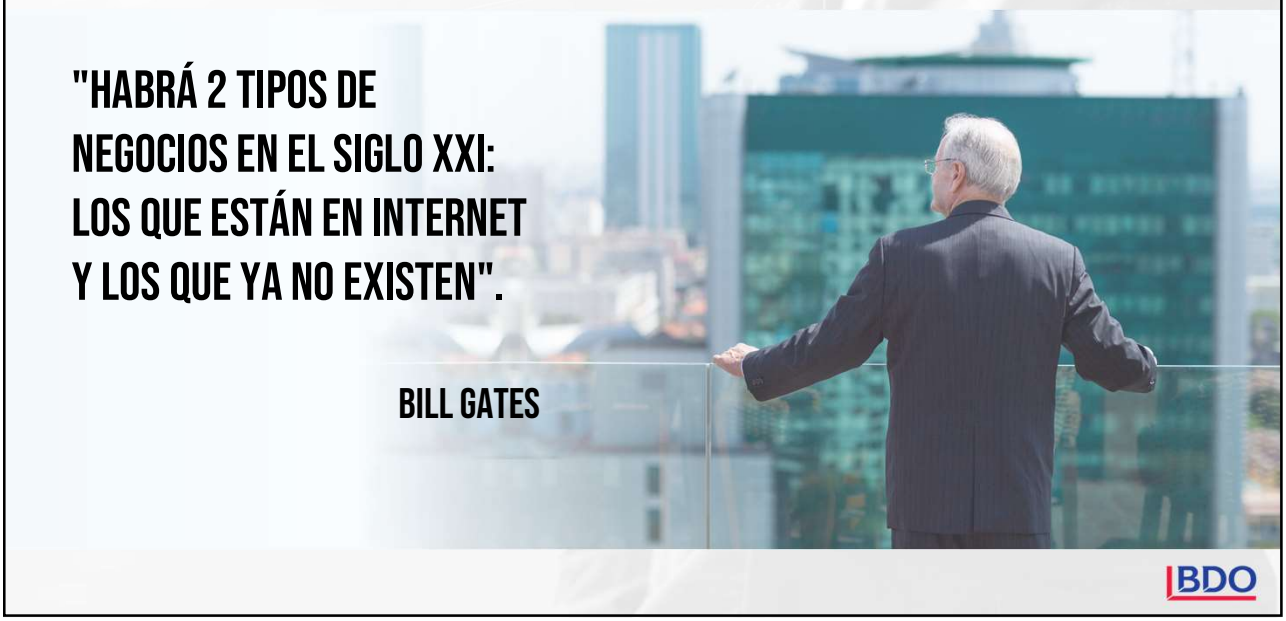
CSX Cybersecurity Proffesional (ISACA Buenos Aires Chapter), Implementer ISO/IEC 31000 (TÜV Rheinland), Lead Auditor ISO/IEC 22301:2019 (Certificate Number 19-3478 - TÜV Rheinland), COBIT5 Foundation (Certificate Number 02363587-01-2EVV - APMG International), Lead Auditor ISO/IEC 20000:2011 (Certificate Number 17-6510 - TÜV Rheinland), ISMS Auditor / Lead Auditor ISO/IEC 27001 (Certificate Number IT2566710 - IRCA / TÜV Rheinland), Dirección de seguridad de la información (Universidad CAECE), ITIL® version 3:2011, Certification for Information Management (EXIN License EXN4396338), ITIL® version 3:2011, Certification for Accredited Trainer (EXIN Accreditation), Foundation ISO/IEC 20000-1:2011, Implementación de SGSIT (LSQA - LATU), Internal Audit ISO/IEC 20000:2011, Auditor Interno en SGSIT (LSQA - LATU)

BDO

3

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información



BDO

4

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

PLANIFICACIÓN ESTRATÉGICA Y GRADO DE INNOVACIÓN

BDO

5

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

NECESIDAD DE INNOVACIÓN TECNOLÓGICA

OPORTUNIDADES

- EMPODERAR AL EMPLEADO
- FOCO EN EL CLIENTE
- EXCELENCIA OPERATIVA
- INNOVACIÓN EN LOS NEGOCIOS
- TRANSFORMACIÓN Y EXCELENCIA IT

¿ESTAMOS PREPARADOS?

RIESGOS

- CONTROL INTERNO
- DATOS / INFORMACIÓN
- GESTIÓN
- CUMPLIMIENTO
- PROCESOS DE NEGOCIO

BDO

6

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

- ¿CUÁL ES EL IMPACTO DE LAS BRECHAS DE CIBERSEGURIDAD EN LAS EMPRESAS?
- ¿CUÁNTO DEBE INVERTIR UNA EMPRESA EN CIBERSEGURIDAD?

LA NECESIDAD DE INNOVACIÓN SE HA CONVERTIDO EN UN FACTOR DE RIESGO AMPLIANDO LA BRECHA DE SEGURIDAD Y CUMPLIMIENTO EN LAS ORGANIZACIONES

BDO

7

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

¿QUE CAMBIÓ CON LA TRANSFORMACIÓN DIGITAL?

- Los Datos no están bajo el control total
- La infraestructura ya no es propia
- Las personas requieren la información cuando y desde donde quieran
- Las economías digitales exigen Interconexión con el Mundo
- Explosión de dispositivos conectados a la red
- Aplicación de la normatividad sin limitar la estrategia digital
- La identidad digital de las personas impacta el negocio
- La marca está expuesta al mundo en redes sociales
- No hay frontera entre la información personal y la corporativa

- La tecnología te permite predecir
- El negocio requiere agilidad y la seguridad no puede ser un obstáculo
- La cultura digital implica cultura de seguridad

BDO

8

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

¿QUE NECESIDAD TIENE NUESTRO CLIENTE?

- Como protejo la información si las fronteras del mundo digital no existen
- Como aseguro las cosas conectadas
- Como incorporo seguridad en las arquitecturas digitales de referencia
- Como hago seguridad social
- Como monitoreo que sucede afuera
- Como protejo la marca en el mundo digital
- Como valoro los riesgos en el mundo digital
- Como protejo infraestructura en la nube que no son propias
- Como genero ROI en el aseguramiento de la arquitectura digital
- Como aseguro el BIG DATA

SENTIR TRANQUILIDAD DE QUE SE CONOCEN LOS RIESGOS, QUE HAY UN TRATAMIENTO ADECUADO DE ELLOS Y SE SABE QUE HACER EN CASO DE UN INCIDENTE DE SEGURIDAD

BDO

9

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

Estratégico

- Fallas del gobierno corporativo y control interno
- Acciones legales o punitivas por falta de cumplimiento al marco regulatorio
- Incapacidad para atraer y retener conocimientos y competencias durante la transición

Operativo y Cumplimiento

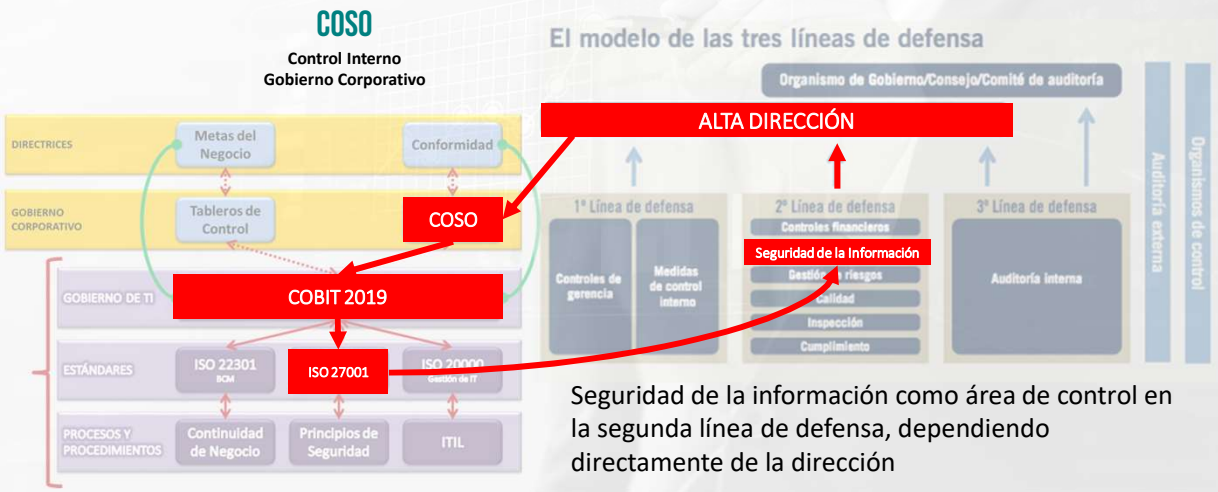
- Administración ineficiente o fallas en la prestación de servicios IT
- Débil seguridad de los datos y mayores riesgos de privacidad
- Incapacidad de explotar y proteger activos (piratería y derechos de propiedad intelectual)
- Sistemas y procesos inadecuados para sustentar el negocio

BDO

10

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información



Seguridad de la información como área de control en la segunda línea de defensa, dependiendo directamente de la dirección

11

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

12

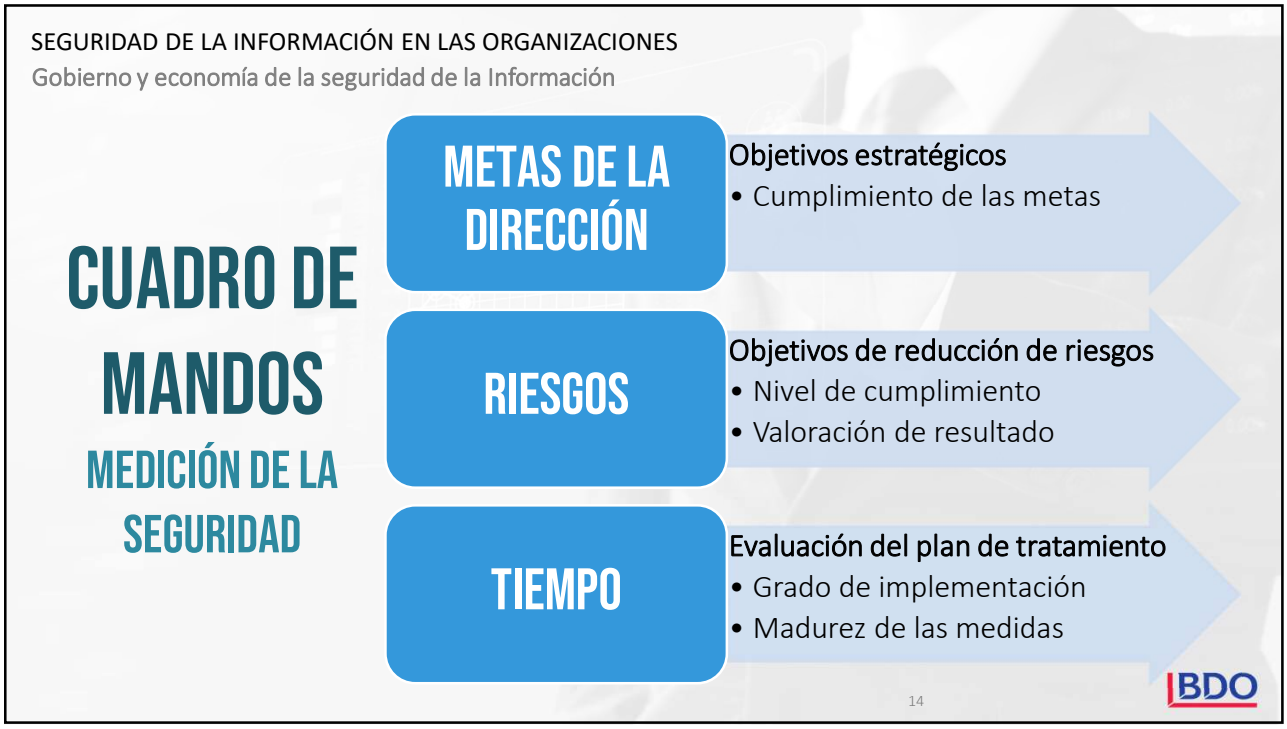
SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

13

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información



14

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

15

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

OBJETIVOS ESTRATÉGICOS DE NEGOCIO Y SU RELACIÓN CON SERVICIOS DE TI Y SEGURIDAD

Financiera	Aumentar la Rentabilidad	Incrementar la cartera con Clientes Nuevos	Aumentar Venta	Crear Nuevos Servicios
Servicios IT	Optimización de la gestión de licenciamiento	Mejora de los presupuestos de IT	Gestión de Proveedores	Planificación e Implementación de Servicios Nuevos o Modificados
Servicios SI	Cumplimiento	Organización interna	Gestión de la entrega de servicio a terceras partes	Procedimientos y responsabilidades operativas
Clientes	**Minimizar los tiempos de atención a solicitudes del cliente**	**Funcionalidad, Adaptación de Servicios a sus Necesidades**	**Precio competitivos**	**Imagen, Desarrollar la Marca como sinónimo de confiabilidad, Prestigio, Reconocimiento**
Servicios IT	Implementación de herramientas tecnológicas de atención al público	Gestión de Nivel de Servicio	Gestión de la operación de CPD y aplicaciones	Gestión de continuidad y disponibilidad del servicio
Servicios SI	Correcto procesamiento en las aplicaciones	Clasificación de la información	Terceras Partes	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
Procesos Internos	**Acelerar la atención de los reclamos, Gestión del cliente, Post-Venta**	**Proceso Mercadeo y Ventas, Identificar necesidades de los clientes**	**Actividades de Mejora Continua para la operación del negocio**	**Mejorar los costos a partir de la selección de proveedores de productos de tecnología de punta**
Servicios IT	Gestión de Nivel de Servicio	Software de gestión CRM + ERP	Gestión de Incidentes Gestión de Problemas	Monitorización de servicios de IT
Servicios SI	Gestión de Resguardos Magnéticos	Planificación y aceptación de sistemas	Gestión de los incidentes de la seguridad de la información	Gestión de las vulnerabilidades técnicas
Aprendizaje y Crecimiento	**Capacitación y Certificación del Personal**	**Implementación y Capacitación de Software de Gestión / CRM - ERP**	**Adquisición y actualización tecnológica**	**Adopción de estándares para el Gobierno Corporativo**
Servicios IT	Gestión del Conocimiento	Calidad de Servicios de IT	Evaluaciones y Auditorías	Sistema de Gestión de Servicios TI ISO20000
Servicios SI	Seguridad de los Recursos Humanos	Protección Física y Ambiental	Evaluaciones y Auditorías	Sistema de Gestión de Seguridad de la Información / ISO27000

BDO

16

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

Necesidades del Negocio = **Necesidades de los Procesos Tecnológicos**

OBJETIVOS ESTRATÉGICOS		
NEGOCIO	**TECNOLOGÍA INFORMÁTICA**	**SEGURIDAD DE LA INFORMACIÓN**
Aumentar la Rentabilidad	Optimización de la gestión de licenciamiento	Cumplimiento legal Integridad de datos Disponibilidad operativa
Cuidado de Imagen Aumento de Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (tercerizados)	Gestión de la entrega de servicio de terceras partes
Acelerar la atención de los reclamos, Gestión del cliente, Atención al cliente, Post-Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (interno)	Gestión de las vulnerabilidades técnicas y gestión de incidentes de seguridad
Mejorar los costos a partir de la selección de proveedores de productos de tecnología de punta	Implementación de herramientas tecnológicas en nuevos proyectos para el Negocio	Aceptación de sistemas de acuerdo al marco regulatorio del Negocio
Optimización de recursos asociados a IT	Gestión de la operación de CPD	Clasificación de la información
Actividades de Mejora Continua para la operación del negocio	Gestión de continuidad y disponibilidad del servicio	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

17

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

El costo promedio de un incidente que involucra servicios de la banca en línea es de US$1.754.000

El 61% de los incidentes de ciberseguridad que afectan a las transacciones bancarias en línea conlleva costos adicionales para la institución afectada, entre ellos la pérdida de datos, pérdida de reputación de la marca o de la compañía, filtración de información confidencial y más.

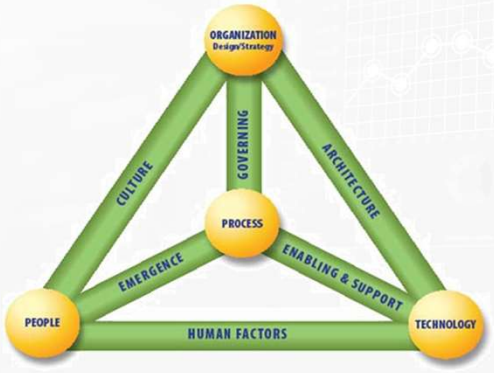
Fuente: Kaspersky Lab / Agosto 2021

18

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

NECESITAMOS TECNOLOGÍA, PERSONAS Y PROCESOS PARA TENER UNA ESTRATEGIA DE SEGURIDAD EXITOSA



INTEGRADO EN COBIT 5 (10/04/2012)

- Compromiso de la Alta Dirección con las iniciativas de seguridad de la información
- Comprensión de la administración de los problemas de seguridad de la información
- Planificación de la seguridad de la información antes de la implementación de nuevas tecnologías
- Integración entre el negocio y la seguridad de la información
- Alineación de la seguridad de la información con los objetivos de la organización

Fuente: Elementos críticos del éxito del programa de seguridad de la información, ISACA, 2005

19

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

- Establecer misión, visión y directrices
- Definir estrategias, modelar y simular
- Evaluar estado y definir nivel de madurez
- Definir organización y dar responsabilidades ejecutivas
- Planificar la comunicación
- Planificar el control
- Definir políticas

20

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

21

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

Este tipo de estudios no es posible realizarlo **sin conocer de forma exhaustiva las amenazas** que afectan a una organización. Para realizarlo de la forma más precisa posible (siempre son estimaciones probabilísticas) debemos remontarnos a la historia reciente de la organización y ver **qué incidentes se han sufrido**, para así poder prever los posibles incidentes futuros y después calcular el **costo asociado a ellos**.

BDO

22

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

EVALUACIÓN CUANTITATIVA DEL RIESGO

EXPECTATIVA DE PÉRDIDA SIMPLE (SLE)

Cantidad esperada de dinero que se pierde cuando se produce un riesgo (costo total de un incidente)

→ Se trata de pérdidas directas (tiempo de inactividad del sitio web, reemplazo de hardware, reemplazo de la pérdida de datos, etc.) y el costo de los daños indirectos (tiempo de investigación, la pérdida de reputación, el impacto en la imagen, etc.)

FRECUENCIA ANUAL DEL RIESGO (ARO)

Medida de la probabilidad de que un riesgo se produce en un año

→
- La ARO de una inundación dependerá de factores geográficos
- La ARO de un fallo en el disco está influenciada por la temperatura de funcionamiento
- La ARO de un robo dependerá de la ubicación de la de activos, etc

EXPECTATIVA DE PERDIDA ANUAL (ALE)

Pérdida monetaria anual que se puede esperar de un riesgo específico sobre un activo específico

→ **ALE = ARO X SLE**

BDO

23

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

EL MODELO GORDON-LOEB

The Economics of Information Security Investment (2002)

El modelo Gordon-Loeb es un modelo económico matemático que analiza el nivel óptimo de inversión en seguridad de la información. Para redactar este modelo, la empresa debe poseer conocimiento de tres parámetros:

- **Cuánto valen los datos (VA – Valor del activo);**
- **Cuánto están en riesgo los datos (FE – Factor de exposición);**
- **La probabilidad de que un ataque a los datos tenga éxito, o vulnerabilidad (ARO – Tasa de ocurrencia anualiazda)**

Estos tres parámetros se multiplican para proporcionar la pérdida de dinero media sin inversión en seguridad. La cantidad de dinero que una empresa gasta en proteger la información debería ser solo una pequeña fracción de la pérdida prevista que según el modelo de Gordon y Loeb no supera el 37%.

- **Ejemplo:** Suponga un valor de datos estimado de **1.000.000 USD**, con una **probabilidad de ataque del 15%** y una **probabilidad del 80% de que un ataque tenga éxito**. En este caso, la pérdida potencial viene dada por el producto **1.000.000 USD × 0,15 × 0,8 = 120.000 USD**. Según Gordon y Loeb, la inversión de la empresa en seguridad no debería superar los **120.000 USD × 0,37 = 44.000 USD**.

BDO

24

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

DEFINICIÓN DEL ALCANCE Y LOS ACTIVOS INVOLUCRADOS EN LA OPERACIÓN DEL PROCESO

Alcance	Activos	Valor	Porcentaje del valor total
Servicio de *hosting*	Servidor de aplicaciones	$ 17,000.00	3%
	Servidor de base de datos	$ 10,000.00	1%
	Conexión a Internet	$ 12,000.00	2%
	Intangibles	$ 15,000.00	2%
	Salarios	$ 25,000.00	4%
	Licencias	$ 100,000.00	15%
	Propiedad intelectual	$ 500,000.00	74%
	Costo total	**$ 679,000.00**	**100%**

SELECCIÓN DEL ACTIVO CRÍTICO

Activo		x 1h	x 24h	X Año
Servidor de aplicaciones	Ventas promedio	$100	$2,400	$876,000

IDENTIFICACIÓN DE AMENAZAS Y PROBABILIDAD DE OCURRENCIA

Amenazas	ARO
Infección por virus (1 vez cada 2 años)	50%
Falla eléctrica (1 veces cada 3 años)	33%
Factor humano intencional (1 vez cada 4 años)	25%
Factor humano no intencional (nunca)	0%

IDENTIFICACIÓN DEL FACTOR DE EXPOSICIÓN

Factor de exposición	Porcentaje
El sistema tiene redundancia o respaldos	30%
El sistema está detrás de un firewall de red	10%
El sistema cuenta con software antivirus instalado	10%
El sistema cuenta con las últimas actualizaciones instaladas	40%
El sistema cuenta con un firewall de host instalado	30%

25

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

Activo	Amenaza	VA	FE	ARO	ALE
Servidor de aplicaciones	Infección por virus (1 vez cada 2 años)	$ 17,000.00	20%	50%	$ 1,700.00

- **VALOR DEL ACTIVO (VA): $17,000.00**
- **FACTOR DE EXPOSICIÓN (FE): 20% (PORCENTAJE DE PÉRDIDA DE ACTIVO CAUSADA POR LA AMENAZA)**
- **TASA ANUALIZADA DE OCURRENCIA (ARO): 50% (1 VEZ CADA DOS AÑOS)**

26

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

MÉTRICA DE GESTIÓN DE RIESGOS CONOCIDA COMO ALE

Pérdida monetaria anual que se puede esperar de un riesgo específico sobre un activo específico

PÉRDIDA POTENCIAL

- LOS VALORES PROBABLES DEL IMPACTO MONETARIO (EXPECTATIVA DE PÉRDIDA)
- LA FRECUENCIA ANUAL DE OCURRENCIA PARA CADA TIPO DE INCIDENTE

VALORES ESTIMADOS CON Y SIN MITIGACIÓN

- ESTADO DE SEGURIDAD ORIGINAL SIN TRATAR
- ESTADO DE SEGURIDAD TRATADO CON SALVAGUARDAS ADECUADAS

BDO

27

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

VALORES PARA ANÁLISIS DE ROSI		
Pérdidas anuales por incidentes sin tratar	$ 200.000,00	→ GESTIÓN DE INCIDENTES
Pérdidas anuales por incidentes mitigados	$ 50.000,00	→ GESTIÓN DE RIESGOS + PLAN
Ahorro bruto anual por controles	**$ 150.000,00**	
Costo inicial de implementación de controles	$ 120.000,00	→ GESTIÓN DE CONTROLES
Costos anuales operacionales de controles	$ 10.000,00	

CALCULO DE ROSI					
ROSI estimado a tres años		0	1	2	3
Ahorro bruto anual por controles			$ 150.000,00	$ 150.000,00	$ 150.000,00
Ahorro bruto anual por controles a valor actual (valor disminuye por acción de las medidas tomadas)			**$ 125.000,00**	**$ 104.166,67**	**$ 86.805,56**
Valor de controles (suma de ahorro anual a valor actual)	**$ 315.972,23**		$ 125.000,00	$ 229.166,67	**$ 315.972,23**
Costo inicial de controles		$ 120.000,00			
Costos anuales operacionales de controles			$ 10.000,00	$ 10.000,00	$ 10.000,00
Costo de controles a valor actual (valor disminuye por acción de las medidas tomadas)		**$ 120.000,00**	**$ 8.333,33**	**$ 6.944,44**	**$ 5.787,04**
Costo de controles (suma de controles a valor actual)	**$ 141.064,81**				
ROSI (%) = (VALOR - COSTO) / COSTO	**124%**	**-$ 120.000,00**	**$ 116.666,67**	**$ 97.222,23**	**$ 81.018,52**
Valor actual neto (VALOR - COSTO)	**$ 174.907,42**				
Tasa interna de rentabilidad de los controles (COSTO INICIAL DE CONTROLES / VALOR ACTUAL NETO)	**69%**	El valor objetivo debe superar el 20% de rentabilidad de los controles			
Plazo de recuperación (valor actual neto > costo de controles)	**Al 1er año**				
Descontando	**Al 2do Año**				

BDO

28

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

	OBJETIVOS ESTRATÉGICOS			RESPUESTA SI		FRECUENCIAS				
Ítem	NEGOCIO	TECNOLOGÍA INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN	Proyectos/Actividades de Seguridad de la Información asociados a los objetivos de Negocio y TI	Impacto negativo en la falta de gestión	Período de medición	Frecuencia de la recolección de datos	Frecuencia del análisis de datos	Frecuencia del reporte del resultado de las mediciones	Revisión de la medición
1	Aumentar la Rentabilidad	Optimización de la gestión de licenciamiento	Cumplimiento legal Integridad de datos Disponibilidad operativa	1. Implementación de herramienta de gestión de software (p.e. Altiris, Fix IQ) 2. Desarrollo de estándares técnicos de configuración de seguridad en plataformas 3. Configuración de GPO y políticas locales en WS para no permitir la instalación de SFW desautorizado 4. Revisión anual de licenciamiento	Multas por no-cumplimiento Riesgo de virus, malware, etc. por instalación de software no autorizado Deficiencia en [illegible] funcionamiento			Mensual	Mensual	Semestral
2	Cuidado de Imagen Aumento de Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (tercerizados)	Gestión de la entrega de servicio de terceras partes	Revisión periódica de proveedores críticos de IT para: 1. Verificar cumplimiento de requisitos normativos relacionados con la seguridad y la operación de los sistemas (SLAs acordados) 2. Verificar condiciones de seguridad asociadas a la disponibilidad de los servicios de IT	Incumplimiento [illegible] los servicios co[illegible] Organización (a[illegible] legales), ya que solidario" en: -> Tratamiento -> Continuidad -> Cumplimient					
3	Acelerar la atención de los reclamos, Gestión del cliente, Atención al cliente, Post-Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (interno)	Gestión de las vulnerabilidades técnicas y gestión de incidentes de seguridad	1. Implementación de solución de antivirus 2. Mantenimiento anual y actualización de BD de antivirus 3. Implementación de celula de respuesta ante incidentes de seguridad	Fuga de inform Indisponibilida Riesgo de integ información en			Mensual	Mensual	Semestral
4	Mejorar los costos a partir de la selección de proveedores de productos de tecnología de punta	Implementación de herramientas tecnológicas en nuevos proyectos para el Negocio	Aceptación de sistemas de acuerdo al marco regulatorio del Negocio	Participación en reuniones de proyecto desde diseño para: 1. Resguardo del cumplimiento normativo y legal en todos los componentes del proyecto 2. Recomendación sobre herramientas o configuraciones para el resguardo de la seguridad 3. Recomendaciones sobre implementación sin perjudicar la operación	Costos adiciona adicionales Falta de cumpli elección de las Multas por no-c Problemas de [illegible] ante implementaciones técnicas no contempladas					

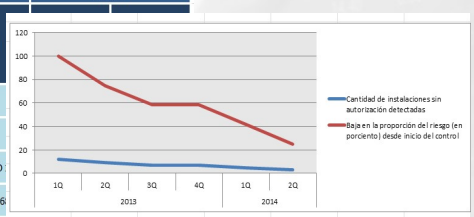
VARIABLES DE MEDICIÓN		
Función de medición SI	Inversión en SI	Valoración de impacto negativo en el Negocio
Licencias registradas e instaladas vs Licencias autorizadas no-autorizadas	U$S 21.000 (solución de appliance FixIQ + H/H mensuales x 1 año en controles)	U$S 68.132 (multa de 3.000 días en sueldo mínimo de U$S 500 - 22 días laborales)
Cantidad de observaciones no-conformes por proveedor en auditorías periódicas	U$S 1.000 (H/H mensuales x 1 año en controles)	U$S 100.000 (base incumplimiento de Ley de Habeas Data) riesgo anual

29

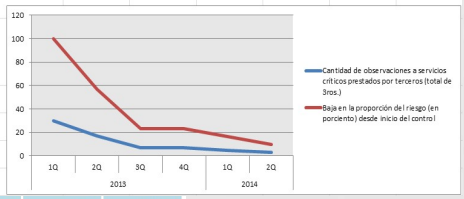
SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

1				2013				2014	
NEGOCIO	TECNOLOGÍA INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN		1Q	2Q	3Q	4Q		
Aumentar la Rentabilidad	Optimización de la gestión de licenciamiento	Cumplimiento legal Integridad de datos Disponibilidad operativa	Cantidad de instalaciones sin autorización detectadas	12	9	7			
			Baja en la proporción del riesgo (en porciento) desde inicio del control	100	75	58			
			Distribución de la inversión/costo en el período	USD 1.750	USD 1.750	USD 1.750	USD		
			Pérdida por multas en caso de materialización del impacto	USD 68.182	USD 68.182	USD 68.182	USD 6		



2				2013					
NEGOCIO	TECNOLOGÍA INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN		1Q	2Q	3Q	4Q		
Cuidado de Imagen Aumento de Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (tercerizados)	Gestión de la entrega de servicio de terceras partes	Cantidad de observaciones a servicios críticos prestados por terceros (total de 3ros.)	30	17	7			
			Baja en la proporción del riesgo (en porciento) desde inicio del control	100	57	23			
			Distribución de la inversión/costo en el período	USD 1.000	USD 1.000	USD 1.000	USD		
			Pérdida por multas en caso de materialización del impacto	USD 33.000	USD 33.000	USD 33.000	USD 33.000	USD 33.000	USD 33.000



30


SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES
Gobierno y economía de la seguridad de la Información
1
INDICADORES CLAVE
METAS DE DIRECCIÓN
Valoración de activos y Análisis de Impacto en los Negocios (BIA)
Expectativa de pérdida anual (ALE)
COBIT 2019
ISO 27016
ISO 22317
2
INDICADORES DE PROGRESO
METAS DE RIESGOS
BIA + definiciones de riesgos corporativos
Riesgo puro, mitigación y riesgo residual (Cuantificable)
ISO 27005
ISO 31000/10
NIST 800-53 V4
3
INDICADORES DE DESEMPEÑO
METAS DE CONTROLES
Definición de indicadores y métricas
Controles Aceptables
ISO 27002
ISO 27004
ISO 27035
BDO

31


GOBIERNO DE SEGURIDAD, TECNOLOGÍA E INFORMACIÓN EN EL NEGOCIO
CONCLUSIÓN
BDO

32

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

¿QUÉ DEBE DOMINAR EL CEO ACERCA DE CIBERSEGURIDAD?

EL GOBIERNO ASEGURA QUE LA ESTRATEGIA DEL NEGOCIO SE MANTIENE CONSISTENTE CON LAS METAS DEL NEGOCIO

BASAR LAS DECISIONES DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y TECNOLOGÍA SOBRE LAS CONSECUENCIAS POTENCIALES AL NEGOCIO

MARCO INTERNO DE CUMPLIMIENTO Y COMUNICACIONES PARA PROTEGER EL NEGOCIO

DOMINAR UNA ESTRATEGIA PARA QUE TUS EMPLEADOS SEAN VIGÍAS Y AGENTES PARA PREVENIR CUALQUIER RIESGO EN TU COMPAÑÍA

SABER LOS RIESGOS QUE IMPLICA NO CUMPLIR CON MANDATOS LEGALES Y REGULATORIOS SOBRE LOS DATOS

CONOCER EL NIVEL DE MADUREZ RESPETO DE CIBERSEGURIDAD CON LA QUE CUENTA TU EMPRESA

BDO

33

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

¿QUÉ DEBE DOMINAR EL CISO ACERCA DEL NEGOCIO?

CISM Certified Information Security Manager

- Entender el gobierno de seguridad de la información, en qué consiste y cómo se logra.
- Entender Estrategia de seguridad de la información
- Entender el significado, el contenido, la creación y el uso de políticas
- Desarrollar casos de negocio y obtener el compromiso del personal directivo.
- Definir requisitos de métricas de gobierno

CRITERIO ESTRATÉGICO APLICABLE AL ENTORNO

PENSAMIENTO EN PROCESOS Y LÍDERES

CONOCIMIENTO DEL NEGOCIO

CONOCIMIENTO DE LOS PROCESOS DE NEGOCIO Y SUS OBJETIVOS

CONOCIMIENTO DE LA TECNOLOGÍA APLICABLE

CONOCIMIENTO DE LAS METODOLOGÍAS APLICABLES

BDO

34

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

CISM Certified Information Security Manager

An ISACA® Certification

HTTPS://ISACA.ORG.AR/CERTIFICAR/CISM-CERTIFIED-INFORMATION-SECURITY-MANAGER/

Certificación única de gestión focalizada en el gobierno de seguridad de la información, la que ha sido obtenida por más de 16.000 profesionales desde su introducción en 2003, indicada para la persona que gestiona, diseña, supervisa y evalúa la seguridad de la información empresarial y que tienen experiencia en las siguientes áreas:

- Gobierno de Seguridad de la Información
- Gestión de Riesgos de Información
- Programa de Desarrollo de Seguridad de la Información
- Programa de Gestión de Seguridad de la Información
- Manejo de Incidentes y Respuesta

BDO

35

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Gobierno y economía de la seguridad de la Información

PENSAR EN SEGURIDAD Y GOBIERNO TECNOLÓGICO DESDE LAS NECESIDADES DEL NEGOCIO ASEGURA LA CONFIANZA DIGITAL PARA LA INNOVACIÓN Y LA TRANSFORMACIÓN DIGITAL

BDO

36


NIST
CLOUD
BIA
ISO20000
BCRA
EVALUACIÓN Y AUDITORÍAS
SANS
BYOD
COBIT5
SWIFT Security Framework
GOBIERNO
RIESGOS Y CUMPLIMIENTO
IOT
CIBERSEGURIDAD
PRIVACIDAD DE DATOS
CONSULTORÍA TI
GESTIÓN DE LA CONTINUIDAD
COMPLIANCE
PCI-DSS
ISO27001
GESTIÓN DE INCIDENTES
COSO
ISAE3402
ERP
ITIL
BCP
ISO38500
SERVICIOS GESTIONADOS
Pablo Silberfich
Socio
psilberfich@bdoargentina.com
Fabián Descalzo
Director
fdescalzo@bdoargentina.com
API
Aseguramiento de Procesos Informáticos
RAS | Risk Advisory Services | IT Assurance, Audit and Compliance
BDO

37