

PRESENTACIÓN INFOSECURITY 2015

BDO: ASEGURAMIENTO DE PROCESOS INFORMÁTICOS (API)

Ing. Pablo A. SILBERFICH

Nuestro equipo está integrado por profesionales especializados en TI al servicio del negocio, con certificaciones CISA, CISM, CISSP, CEH, entre otros.

PRODUCTO / SERVICIO: AUDITORÍA Y CONSULTORÍA INFORMÁTICA



NUESTROS SERVICIOS

Auditoría

**(Interna, Externa y
Certificaciones - Homologaciones,
Computación Forense)**

Consultoría

**(Tecnología Informática, Sistemas, Aplicaciones, Comunicaciones
y Seguridad de la Información)**

Tercerización

(Servicios de «collocation» de RRHH y/o soporte)

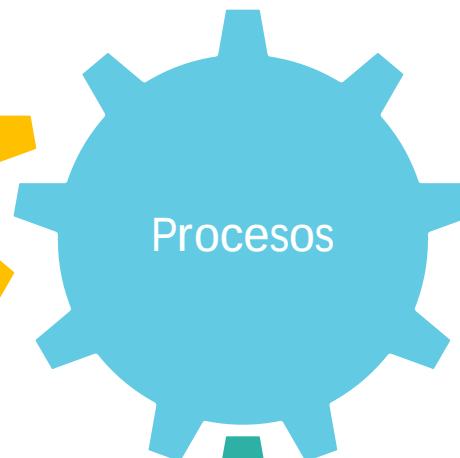


BENEFICIOS CONCRETOS PARA NUESTROS CLIENTES

Seguridad de la
Información



Personas



Procesos

Administración
de TI



Productividad

Calidad de
Servicio de TI



Costos

Enfoque de
Negocio

AUDITORÍA DE SISTEMAS

Auditorías de sistemas y aplicativos bajo marcos de referencia y estándares internacionales (COBIT, GTAGs) y nacionales (BCRA 4609, 5374) y otros.



EJEMPLOS DE NUESTROS SERVICIOS - AUDITORIA

Servicio Auditoría Interna de Sistemas



**Prevenir....
Evitar Multas / Sanciones / Fraudes**

¿CÓMO PODEMOS AYUDARLO? (cont.)

CONSULTORÍA EN SISTEMAS Y CONTROL DE PROYECTOS

Asesoramiento y consultoría en áreas de TI.

Planificación estratégica de TI.

Análisis y gestión de riesgos de TI basado en Magerit 2.

Consultoría en estándares nacionales e internacionales como ITIL, ISO 20.000, COBIT, BCRA 4609, BCRA 5374.

Análisis de factibilidad de proyectos de sistemas.

Consultoría en controles de aplicaciones y procesos de áreas de TI.

Gerenciamiento y control de proyectos informáticos.

Desarrollo de RFP's y selección de sistemas.

Proyectos de Business Intelligence, Data Warehouse, Datamart y Data Mining.

Seguridad en E-Commerce.

Comunicación “A” 4609 del BCRA para entidades Financieras

- Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

ISO/IEC 27001, 27005

- Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)

Basilea II

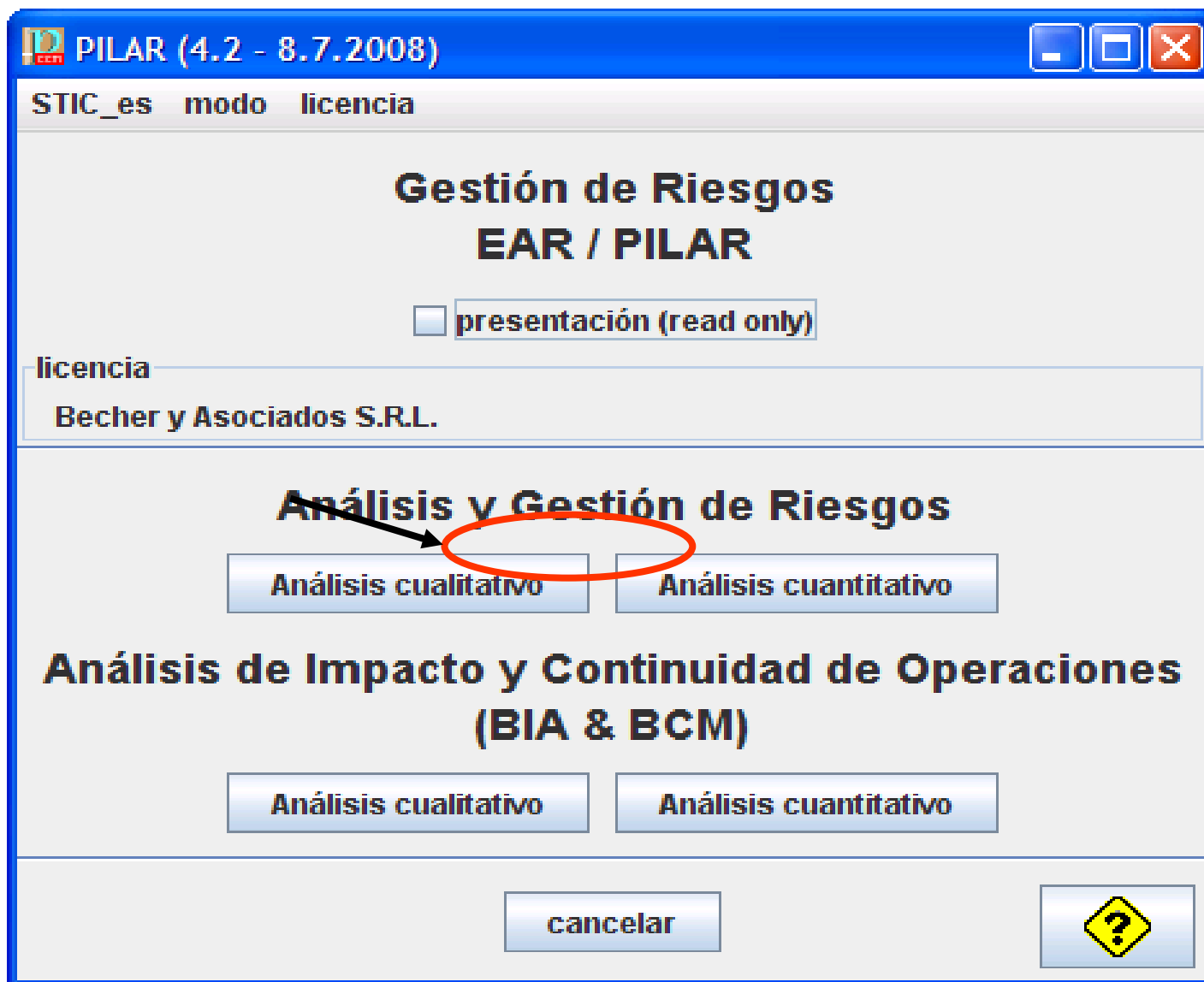
- Estandar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

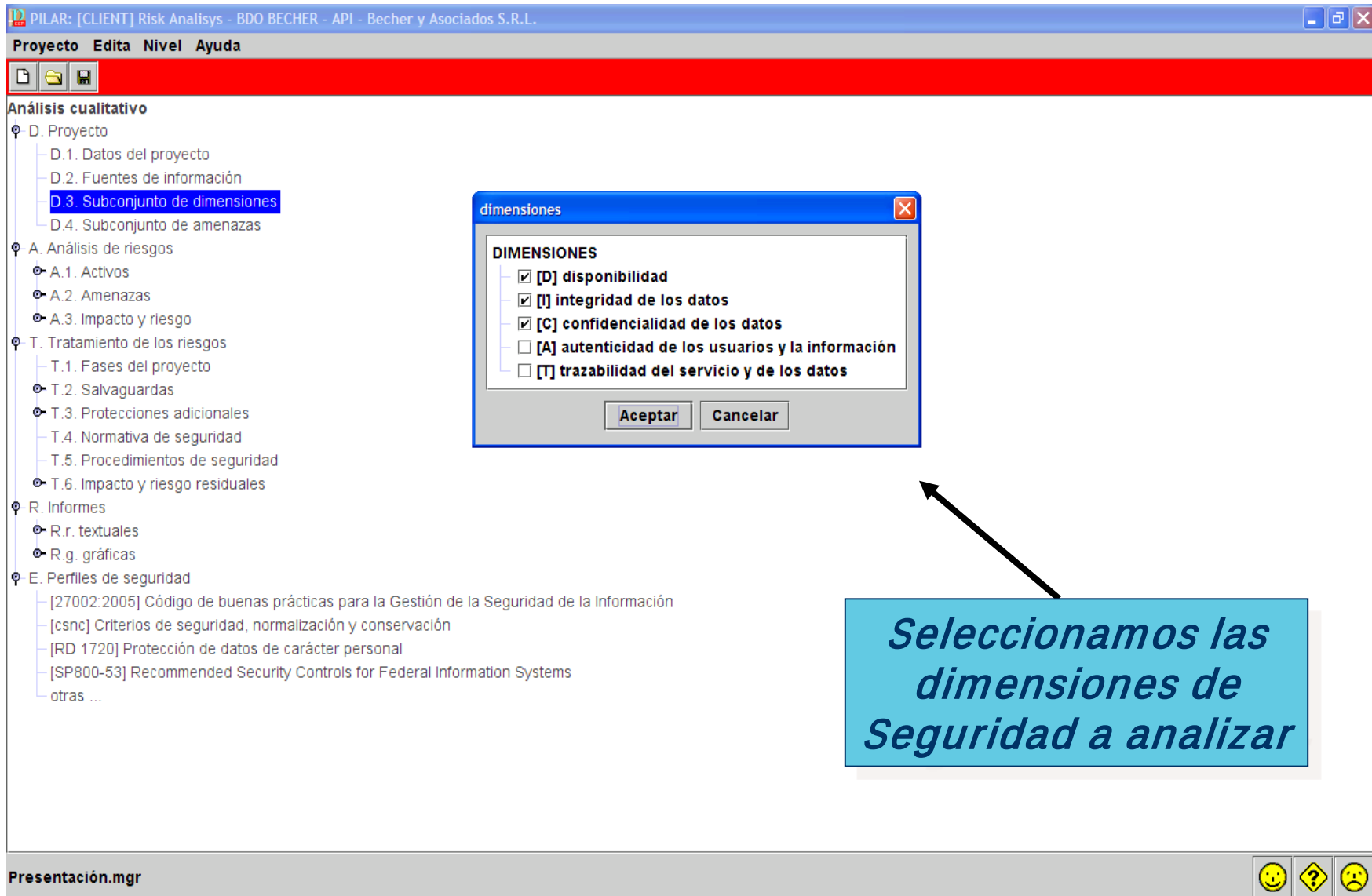
Ley Sarbanes Oxley (SOX)

- Impulsada por el gobierno norteamericano como respuesta a los mega fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros.

ISO/IEC 27005

- 1. Establecer el contexto.**
- 2. Evaluación del riesgo.**
 - a. Identificación del riesgo**
 - b. Estimación del riesgo**
 - c. Valoración del riesgo**
- 3. Tratamiento del riesgo.**
- 4. Aceptación del riesgo.**
- 5. Comunicación del riesgo.**
- 6. Seguimiento del riesgo.**





biblioteca: std: Subconjunto de amenazas - Becher y Asociados S.R.L.

AMENAZAS

- ⚠ [N] Desastres naturales
 - ⚠ [N.1] Fuego
 - ⚠ [N.2] Daños por agua
 - ⚠ [N.*] Desastres naturales
 - ⚠ [N.*.1] Tormentas
 - ⚠ [N.*.2] Tormentas eléctricas
 - ⚠ [N.*.3] Huracanes
 - ✖ [N.*.4] Terremotos
 - ⚠ [N.*.5] Tornados
 - ⚠ [N.*.6] Ciclones
 - ✖ [N.*.7] Deslizamientos del terreno
 - ✖ [N.*.8] Meteoritos
 - ✖ [N.*.9] Tsunamis
 - ⚠ [N.*.10] Tormentas de invierno y frío extremo
 - ⚠ [N.*.11] Calor extremo
 - ✖ [N.*.12] Volcanes
- ⚠ [I] De origen industrial
- ⚠ [E] Errores y fallos no intencionados
 - ⚠ [E.1] Errores de los usuarios
 - ⚠ [E.2] Errores del administrador
 - ⚠ [E.3] Errores de monitorización (log)
 - ⚠ [E.4] Errores de configuración
 - ⚠ [E.7] Deficiencias en la organización
 - ⚠ [E.7.1] No existe procedimiento de atención
 - ⚠ [E.7.2] No hay una persona a cargo
 - ⚠ [E.7.3] Fallo de comunicación
 - ⚠ [E.7.4] No hay registro de lo que ocurre
 - ⚠ [E.8] Difusión de software dañino
 - ⚠ [E.8.0] Gusanos
 - ⚠ [E.8.1] Virus
 - ⚠ [E.8.2] Caballos de Troya
 - ⚠ [E.8.3] Spyware
 - ⚠ [E.9] Errores de [re-]encaminamiento

Grupos de amenazas

se puede eliminar las que no corresponden por su muy baja probabilidad de ocurrencia o frecuencia.

3 on off

CLIENT: identificación de activos - Becher y Asociados S.R.L.

Capas Activos Dominios Estadísticas

ACTIVOS

- [SERVICIOS] SERVICIOS
 - [SERV INT] Servicios Internos
 - [SIMP] SERVICIO DE IMPRESIÓN y FAXES
 - [SRED] SERVICIO DE RED
 - [SINT] SERVICIO DE INTERNET
 - [TELEFONÍA] Servicio de Telefonía (Tel + Cableado Interno)
 - [Serv_MAIL] LOTUS NOTES
 - [SERV CONT] SERVICIOS CONTRATADOS
 - [STEL] SERVICIO DE RED TELEFONÍA
 - [ISP] Proveedor del Servicio de Internet
 - [CPD] SALAS DE CENTRO DE COMPUTOS
 - [CPD] Centro Procesamiento de Datos
- [PRCS] PROCESOS
 - [CRED MIN] CREDITOS MINORISTAS
 - [CRED MIN 1] ORIGINACIÓN DE PRESTAMOS PRENDARIOS
 - [CRED MIN 1.1] Investigación
- [ACT] ACTIVOS TECNOLÓGICOS
 - [HARD PRINCIPAL] HARDWARE PRINCIPAL
 - [SERVERS] Servidores
 - [ARCIFS01] File Server
 - [ARCILN01] Servidor de Correo
 - [ARCIDB01] Servidor Base de Datos
 - [ARCIPS01] Servidor para Impresión
 - [COMM] Equipos de Comunicaciones
 - [HARD SECUNDARIO] HARDWARE SECUNDARIO
 - [PCS] PCS DE ESCRITORIO
 - [IMP] IMPRESORAS Y FAXES
 - [SIST] SISTEMAS APLICATIVOS
 - [FU] FINANCIAR UNIVERSE
 - [APS] Application Processing Systems
 - [LOTUS] LOTUS NOTES

Capas

Se crean los activos a analizar, cada uno corresponde a distintas Capas.

- 3 + dominio fuente

CSV

Caracterización de un activo

Activo: [HARD PRINCIPAL.SERVERS.ARCIFS01] File Server - Becher y Asociados S.R.L.

código
ARCIFS01

nombre
File Server

dato	valor
descripción	File Server y de Aplicaciones
responsable	Gerente de Infraestructura
ubicación	CPD
cantidad	1
propietario	Gerente de Operaciones

sube baja nueva eliminar estándar limpiar

Fuentes de información

dominio
[base.ACT] ACTIVOS TECNOLOGICOS

descripción

CLASES DE ACTIVOS

- ☐ [null] Activos virtuales
- ☒ [S] Servicios
- ☒ [D] Datos / Información
- ☒ [SW] Aplicaciones (software)
- ☒ [HW] Equipamiento informático (hardware)
 - ☐ [host] grandes equipos
 - ☒ [mid] equipos medios
 - ☐ [pc] informática personal
 - ☐ [vhos] equipos virtuales
 - ☐ [cluster] cluster
 - ☐ [mobile] informática móvil
 - ☐ [pda] agendas electrónicas
 - ☐ [easy] fácilmente reemplazables
 - ☒ [data] que almacena datos
 - ☐ [peripheral] periféricos
 - ☐ [bd] dispositivo de front-end
 - ☐ [network] soporte de la red
 - ☐ [pabx] centralita telefónica
 - ☐ [other] otros...
- ☐ [COM] Redes de comunicaciones
- ☒ [Media] Soportes de información
- ☒ [AUX] Equipamiento auxiliar
 - ☐ [power] fuentes de alimentación
 - ☐ [ups] sai - sistemas de alimentación ininterrumpida
 - ☐ [gen] generadores eléctricos
 - ☐ [ac] equipos de climatización
 - ☐ [cabling] cableado
 - ☒ [robot] robots
 - ☐ [supply] suministros esenciales
 - ☐ [destroy] equipos de destrucción de soportes
 - ☐ [furniture] mobiliario
 - ☐ [safe] cajas fuertes
 - ☐ [other] otros...

comentario

activo: ARCIFS01

Server de procesamiento de la aplicación principal, incluye a la Bases de Datos. Posee asociado un robot para realizar los Backup y es servidor de archivos. Se encuentra alojado en el CPD y recibe todas las medidas de seguridad implementadas en el mismo, además posee por cada fuente de alimentación una UPS de 10KVA.

Aceptar Cancelar

Dependencias de los activos

CLIENT: Dependencias entre activos - Becher y Asociados S.R.L.

Exportar Selección Estadísticas

PADRES - 1 + sugiere muestra los hijos HIJOS - 1 + muestra los padres

ACTIVOS

- [SERVICIOS] SERVICIOS
- [CPD] SALAS DE CENTRO DE COMPUTOS
- [PRCS] PROCESOS
- [CRED MIN] CREDITOS MINORISTAS
 - [CRED MIN 1] ORIGINACIÓN DE PRESTAMOS PRENDARIOS
 - [CRED MIN 1.1] Investigación**
 - [SERV INT.SIMP] SERVICIO DE IMPRESIÓN y FAXES
 - [SERV INT.SRED] SERVICIO DE RED
 - [HARD PRINCIPAL.SERVERS.ARCIPS01] Servidor para Impresión
 - [HARD SECUNDARIO.IMP] IMPRESORAS Y FAXES
 - [SERV INT.SINT] SERVICIO DE INTERNET
 - [SERV CONT.ISP] Proveedor del Servicio de Internet
 - [HARD PRINCIPAL.COMM.DTU] DTU
 - [SERV INT.STELEFONÍA] Servicio de Telefonía (Tel + Cableado)
 - [SERV CONT.STEL] SERVICIO DE RED TELEFONÍA
 - [HARD PRINCIPAL.COMM.CTEL] Central Telefonica
 - [SERV INT.Serv_MAIL] LOTUS NOTES
 - [SIST.LOTUS] LOTUS NOTES
 - [HARD SECUNDARIO.PCS] PCS DE ESCRITORIO
 - [SERV INT.SRED] SERVICIO DE RED
 - [SIST.FU] FINANCIAL UNIVERSE
 - [HARD PRINCIPAL.SERVERS.ARCIFS01] File Server
 - [HARD PRINCIPAL.SERVERS.ARCIDB02] Servidor Base de Datos
 - [SIST.APS] Application Processing Systems
 - [HARD PRINCIPAL.SERVERS.ARCIFS01] File Server
 - [HARD PRINCIPAL.SERVERS.ARCIDB02] Servidor Base de Datos
- [ACT] ACTIVOS TECNOLÓGICOS

Microsoft Office Picture Manager

Archivos Edición Ver Imagen Herramientas 2

Escriba una pregunta

Accesos directos...

64%

Editar imágenes... Autocorrección

Diagrama de Dependencias:

```

graph TD
    CRED_MIN_1_1[CRED MIN 1.1] --> STELEFONIA[STELEFONÍA]
    CRED_MIN_1_1 --> SINT[SINT]
    CRED_MIN_1_1 --> FU[FU]
    CRED_MIN_1_1 --> APS[APS]
    CRED_MIN_1_1 --> Serv_MAIL[Serv_MAIL]
    CRED_MIN_1_1 --> PCS[PCS]
    CRED_MIN_1_1 --> SIMP[SIMP]
    STELEFONIA --> STEL[STEL]
    STELEFONIA --> CTEL[CTEL]
    SINT --> DTU[DTU]
    SINT --> ROUTER[ROUTER]
    SINT --> ISP[ISP]
    FU --> ARCIDB02[ARCIDB02]
    FU --> ARCIFS01[ARCIFS01]
    APS --> ARCIFS01
    Serv_MAIL --> LOTUS[LOTUS]
    PCS --> SRED[SRED]
    SIMP --> ARCIFS01
    SIMP --> IMP[IMP]
    STEL --> SW1[SW1]
    CTEL --> SW1
    DTU --> FW[FW]
    ROUTER --> FW
    ISP --> SW1
    ARCIDB02 --> SW1
    ARCIFS01 --> SW1
    ARCIFS01 --> SW1
    ARCIFS01 --> SW1
    ARCIFS01 --> SW1
    ARCIFS01 --> SW1
    SRED --> SW1
    IMP --> SW1
    FW --> SW1
    SW1 --> CPD[CPD]
  
```

Presentación.png

Zoom: 64%

layer_map asset_graph asset_map

aplicar eliminar

CLIENT: valoración de los activos - Becher y Asociados S.R.L.

Edita Exportar Importar

activo	[D]	[I]	[C]
ACTIVOS			
☐ [SERVICIOS] SERVICIOS			
☐ [SERV INT] Servicios Internos			
☐ [SIMP] SERVICIO DE IMPRESIÓN y FAXES	[3]		[7]
☐ [SRED] SERVICIO DE RED	[7]	[7]	[7]
☐ [SINT] SERVICIO DE INTERNET	[5]	[7]	[7]
☐ [STEFONÍA] Servicio de Telefonía (Tel + Cableado Interno)	[5]		[7]
☐ [Serv_MAIL] LOTUS NOTES	[7]	[7]	[7]
☐ [SERV CONT] SERVICIOS CONTRATADOS			
☐ [STEL] SERVICIO DE RED TELEFONÍA	[5]		[7]
☐ [ISP] Proveedor del Servicio de Internet	[5]	[7]	[7]
☐ [CPD] SALAS DE CENTRO DE COMPUTOS			
☐ [CPD] Centro Procesamiento de Datos	[7]	[7]	[7]
☐ [PRCS] PROCESOS			
☐ [CRED MIN] CREDITOS MINORISTAS			
☐ [CRED MIN 1] ORIGINACIÓN DE PRESTAMOS PRENDARIOS			
☐ [CRED MIN 1.1] Investigación	[5]	[7]	[7]
☐ [ACT] ACTIVOS TECNOLÓGICOS			
☐ [HARD PRINCIPAL] HARDWARE PRINCIPAL			
☐ [SERVERS] Servidores			
☐ [COMM] Equipos de Comunicaciones			
☐ [HARD SECUNDARIO] HARDWARE SECUNDARIO			
☐ [PCS] PCS DE ESCRITORIO			[7]
☐ [IMP] IMPRESORAS Y FAXES			[7]
☐ [SIST] SISTEMAS APLICATIVOS			
☐ [FU] FINANCIAR UNIVERSE	[7]	[7]	[7]
☐ [APS] Application Processing Systems	[5]	[7]	[7]
☐ [LOTUS] LOTUS NOTES	[5]	[7]	[7]

Valoración de los activos

- 3 +

acumulado

Identificación de las amenazas

CLIENT: Identificación y valoración de las amenazas - Becher y Asociados S.R.L.

amenazas

AMENAZAS

activos

[ARCIFS01] File Server

- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de [re-]encaminamiento
- [E.10] Errores de secuencia
- [E.14] Escapes de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de información
- [E.20] Vulnerabilidades de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario

AMENAZAS

- [N] Desastres naturales
 - [N.1] Fuego
 - [N.2] Daños por agua
 - [N.*] Desastres naturales
- [I] De origen industrial
 - [I.1] Fuego
 - [I.2] Daños por agua
 - [I.*] Desastres industriales
 - [I.3] Contaminación mecánica
 - [I.4] Contaminación electromagnética
 - [I.5] Avería de origen físico o lógico
 - [I.6] Corte del suministro eléctrico
 - [I.7] Condiciones inadecuadas de temperatura o humedad
 - [I.8] Fallo de servicios de comunicaciones
 - [I.9] Interrupción de otros servicios o suministros esenciales
 - [I.10] Degradación de los soportes de almacenamiento de la información
 - [I.11] Emanaciones electromagnéticas
- [E] Errores y fallos no intencionados
 - [E.1] Errores de los usuarios
 - [E.2] Errores del administrador
 - [E.3] Errores de monitorización (log)
 - [E.4] Errores de configuración
 - [E.7] Deficiencias en la organización
 - [E.8] Difusión de software dañino
 - [E.9] Errores de [re-]encaminamiento
 - [E.10] Errores de secuencia
 - [E.14] Escapes de información
 - [E.15] Alteración de la información
 - [E.16] Introducción de falsa información
 - [E.17] Degradación de la información
 - [E.18] Destrucción de la información
 - [E.19] Divulgación de información

carga biblioteca aplicar eliminar

CLIENT: Valoración de las amenazas - Becher y Asociados S.R.L.

Edita Exportar Importar

	activo	frecuencia	[D]	[I]	[C]
☐ [SERVERS] Servidores					
☐ [ARCIFS01] File Server			100%	100%	100%
☐ [I.1] Fuego		0,5	100%		
☐ [I.2] Daños por agua		0,5	50%		
☐ [I.*] Desastres industriales		0,1	100%		
☐ [I.3] Contaminación mecánica		1	50%		
☐ [I.4] Contaminación electromagnética		1	10%		
☐ [I.5] Avería de origen físico o lógico		1	50%		
☐ [I.6] Corte del suministro eléctrico		1	100%		
☐ [I.7] Condiciones inadecuadas de temperatura o humedad		10	10%		
☐ [I.9] Interrupción de otros servicios o suministros esenciales		1	50%		
☐ [I.10] Degradación de los soportes de almacenamiento de datos		0,1	10%		
☐ [I.11] Emanaciones electromagnéticas		0,1			1%
☐ [E.1] Errores de los usuarios		100	10%	10%	10%
☐ [E.2] Errores del administrador		2	50%	20%	10%
☐ [E.4] Errores de configuración		2	50%	10%	10%
☐ [E.7] Deficiencias en la organización		1	1%		10%
☐ [E.8] Difusión de software dañino		100	10%	10%	10%
☐ [E.9] Errores de [re-]encaminamiento		1		1%	10%
☐ [E.10] Errores de secuencia		0,5		10%	
☐ [E.14] Escapes de información		10			10%
☐ [E.15] Errores de programación		10		1%	
☐ [E.16] Errores de actualización		100		1%	
☐ [E.17] Errores de instalación		10		1%	
☐ [E.18] Errores de migración		10	1%		
☐ [E.19] Errores de programación		1			10%
☐ [E.20] Errores de programas (software)		1	1%	20%	20%
☐ [E.21] Errores de actualización de programas		10	1%	1%	1%
☐ [E.22] Errores de actualización de equipos		1	10%		
☐ [E.23] Errores de mantenimiento de recursos		10			
☐ [E.24] Errores de formación		10			
☐ [E.25] Errores de gestión del usuario		1		50%	50%

Degradación

Valoración de las amenazas

Frecuencia	
1	Una vez al año
2	Dos veces al año
10	Mensual
100	Diario
0.5	Cada 2 años
0.1	Cada 10 años

carga biblioteca eliminar

CLIENT: riesgo acumulado - Becher y Asociados S.R.L.

	activo	[D]	[I]	[C]
☐	ACTIVOS	{8.0}	{8.1}	{8.1}
☐	☞ [SERVICIOS] SERVICIOS	{6.2}	{6.3}	{6.3}
☐	☞ [CPD] SALAS DE CENTRO DE COMPUTOS	{7.7}	{8.1}	{8.1}
☐	☞ [PRCS] PROCESOS			
☐	☞ [ACT] ACTIVOS TECNOLÓGICOS	{8.0}	{8.1}	{8.1}
☐	☞ [HARD PRINCIPAL] HARDWARE PRINCIPAL	{8.0}	{8.1}	{8.1}
☐	☞ [SERVERS] Servidores	{8.0}	{8.1}	{8.1}
☐	☞ [ARCIFS01] File Server	{7.7}	{8.1}	{8.1}
☐	☞ [I.1] Fuego	{6.6}		
☐	☞ [I.2] Daños por agua	{6.0}		
☐	☞ [I.3] Desastres industriales	{5.9}		
☐	☞ [I.3] Contaminación mecánica	{6.3}		
☐	☞ [I.4] Contaminación electromagnética	{5.1}		
☐	☞ [I.5] Avería de origen físico o lógico	{6.3}		
☐	☞ [I.6] Corte del suministro eléctrico	{6.8}		
☐	☞ [I.7] Condiciones inadecuadas de temperatura o humedad	{7.7}		
☐	☞ [I.9] Interrupción de otros servicios o suministros esenciales	{6.3}		
☐	☞ [I.10] Degradación de los soportes de almacenamiento de la inf	{5.9}		
☐	☞ [I.11] Emanaciones electromagnéticas			{2.4}
☐	☞ [E.1] Errores de los usuarios	{6.8}	{6.8}	{6.8}
☐	☞ [E.2] Errores del administrador	{6.6}	{5.9}	{5.3}
☐	☞ [E.4] Errores de configuración	{6.6}	{5.3}	{5.3}
☐	☞ [E.7] Deficiencias en la organización	{3.3}		{5.1}
☐	☞ [E.8] Difusión de software dañino	{6.8}	{6.8}	{6.8}
☐	☞ [E.9] Errores de [re-]encaminamiento		{3.3}	{5.1}
☐	☞ [E.10] Errores de secuencia		{4.8}	
☐	☞ [E.14] Escapes de información			{5.9}
☐	☞ [E.15] Alteración de la información		{4.2}	
☐	☞ [E.16] Introducción de falsa información			
☐	☞ [E.17] Degradación de la información			
☐	☞ [E.18] Destrucción de la información			
☐	☞ [E.19] Divulgación de información			
☐	☞ [E.20] Vulnerabilidades de los programas (software)			
☐	☞ [E.21] Errores de mantenimiento / actualización de programas			

niveles de criticidad

crítico

muy alto

alto

medio

bajo

despreciable

Aceptar

Riesgo intrínseco de cada activo sin considerar las salvaguardas

- 1 + +1 dominio fuente leyenda html csv

CLIENT: Eficacia de las salvaguardas - Becher y Asociados S.R.L.

Edita Exportar Importar

base base.ACT base.PROCS

aspe... estra... comp... salvaguarda

Niveles de madurez

com... reco... curr... target

Se identifican las salvaguardas existentes y se las valoriza en función de la eficacia de la misma

comentario

dominio: [base.ACT] ACTIVOS TECNOLÓGICOS
salvaguarda: Pruebas

Se realizan pruebas sobre las ups y el generador 3 veces por año y se registran los resultados.

Aceptar Cancelar

aplicar rellena predice sugiere cambios

< Lx

CLIENT: riesgo acumulado - Becher y Asociados S.R.L.

potencial current target

activo	[D]	[I]	[C]
ACTIVOS	{2.3}	{2.5}	{2.4}
[SERVICIOS] SERVICIOS	{1.7}	{2.3}	{2.4}
[CPD] SALAS DE CENTRO DE COMPUTOS	{2.1}	{2.4}	{2.4}
[PRCS] PROCESOS			
[ACT] ACTIVOS TECNOLÓGICOS	{2.3}	{2.5}	{2.4}
[HARD PRINCIPAL] HARDWARE PRINCIPAL	{2.3}	{2.5}	{2.4}
[SERVERS] Servidores	{2.3}	{2.5}	{2.4}
[ARCIFS01] File Server	{2.3}	{2.4}	{2.4}
[I.1] Fuego	{0.4}		
[I.2] Daños por agua	{0.4}		
[I.] Desastres industriales	{0.0}		
[I.3] Contaminación mecánica	{0.7}		
[I.4] Contaminación electromagnética	{0.5}		
[I.5] Avería de origen físico o lógico	{0.6}		
[I.6] Corte del suministro eléctrico	{0.8}		
[I.7] Condiciones inadecuadas de temperatura o humedad	{1.6}		
[I.9] Interrupción de otros servicios o suministros esenciales	{0.6}		
[I.10] Degradación de los soportes de almacenamiento de la inf	{0.0}		
[I.11] Emanaciones electromagnéticas			{0.0}
[E.1] Errores de los usuarios	{2.3}	{2.3}	{2.3}
[E.2] Errores del administrador	{0.9}	{0.9}	{0.8}
[E.4] Errores de configuración	{0.9}	{0.8}	{0.8}
[E.7] Deficiencias en la organización	{0.2}		{0.5}
[E.8] Difusión de software dañino			
[E.9] Errores de [re-]encaminamiento			
[E.10] Errores de secuencia			
[E.14] Escapes de información			
[E.15] Alteración de la información			
[E.16] Introducción de falsa información		{2.1}	
[E.17] Degradación de la información		{1.7}	
[E.18] Destrucción de la información	{1.7}		
[E.19] Divulgación de información			{0.5}

niveles de criticidad

- crítico
- muy alto
- alto
- medio
- bajo
- despreciable

Aceptar

Riesgo asociado a cada activo, considerando las salvaguardas

- 1 + -1 dominio fuente gestiona leyenda html csv

CLIENT: riesgo repercutido - Becher y Asociados S.R.L.

potencial	current	target				
			activo	[D]	[I]	[C]
☐			ACTIVOS	{2.3}	{2.5}	{2.4}
☐	☒		[SIMP] SERVICIO DE IMPRESIÓN y FAXES	{1.9}		{2.4}
☐	☒		[SRED] SERVICIO DE RED	{1.8}	{2.3}	{2.4}
☐	☒		[SINT] SERVICIO DE INTERNET	{1.6}	{2.3}	{2.4}
☐	☒		[STELEFONÍA] Servicio de Telefonía (Tel + Cableado Interno)	{1.6}		{2.4}
☐	☒		[Serv_MAIL] LOTUS NOTES	{2.1}	{2.3}	{2.3}
☐	☒		[STEL] SERVICIO DE RED TELEFONÍA	{1.3}		{2.4}
☐	☒		[ISP] Proveedor del Servicio de Internet	{1.3}	{2.3}	{2.4}
☐	☒		[CPD] Centro Procesamiento de Datos	{1.8}	{2.2}	{2.2}
☐	☒		[CRED MIN 1.1] Investigación	{2.0}	{2.3}	{2.4}
☐	☒		[ARCIFS01] File Server	{2.3}	{2.4}	{2.4}
☐	☒		[...] ...			
☐	☒		[CPD] Centro Procesamiento de Datos	{2.1}	{2.4}	{2.4}
☐	☒		[N.1] Fuego	{0.9}		
☐	☒		[N.2] Daños por agua	{0.7}		
☐	☒		[N.*] Desastres naturales	{0.4}		
☐	☒		[I.1] Fuego	{0.9}		
☐	☒		[I.2] Daños por agua	{0.7}		
☐	☒		[I.*] Desastres industriales	{0.7}		
☐	☒		[I.3] Contaminación mecánica	{0.4}		
☐	☒		[I.5] Avería de origen físico o lógico	{0.7}		
☐	☒		[I.6] Corte del suministro eléctrico	{2.1}		
☐	☒		[I.7] Condiciones inadecuadas de temperatura o humedad	{1.6}		
☐	☒		[A.7] Uso no previsto			{2.4}
☐	☒		[A.11] Acceso no autorizado	{1.2}	{1.1}	{1.3}
☐	☒		[A.25] Robo de equipos	{0.5}		{0.6}
☐	☒		[A.26] Ataque destructivo	{0.7}		
☐	☒		[A.27] Ocupación enemiga	{0.7}	{0.6}	{0.6}
☐	☒		[HARD PRINCIPAL.COMM.SW1] Swich 1	{1.8}	{1.1}	{1.2}
☐	☒		[ARCILN01] Servidor de Correo	{2.1}	{2.4}	{2.4}
☐	☒		[ARCIDB02] Servidor Base de Datos	{2.3}	{2.5}	{2.4}
☐	☒		[ARCIPS01] Servidor para Impresión	{1.9}		{2.1}

niveles de criticidad

critico

muy alto

alto

medio

bajo

despreciable

Aceptar

leyenda

html csv

Riesgo Repercutido

EJEMPLOS DE NUESTROS SERVICIOS - CONSULTORÍA

Servicio Seguridad en E-Commerce



EJEMPLOS DE NUESTROS SERVICIOS - CONSULTORÍA

SEGURIDAD DE LA INFORMACIÓN

Podemos brindarle soluciones a su medida, ya que contamos con una amplia experiencia en el área de seguridad de la información, dando servicios de consultoría en las normas de la serie ISO 27000, Ley de Protección de Datos Personales, test de intrusión, [Asesoramiento a Gerencias de Seguridad de la Información \(PESI\)](#), planes de concientización (Awareness), Computación forense, BCP (Business Continuity Plan) y DRP (Disaster Recovery Plan) y otros servicios especializados del área.



PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)

Es un instrumento en donde se refleja secuencialmente y priorizados las políticas, inversiones, recursos y necesidades del negocio relacionadas con la Seguridad de la Información.



Cómo armar e Implementar un PESI?

- 1. Identificar tareas actuales aplicados a S.I.**
- 2. Identificar tiempos asociados a las tareas (1).**
- 3. Identificar tiempos disponibles del personal de S.I.**
- 4. Identificar la capacidad del personal de S.I.**



Cómo armar e Implementar un PESI?

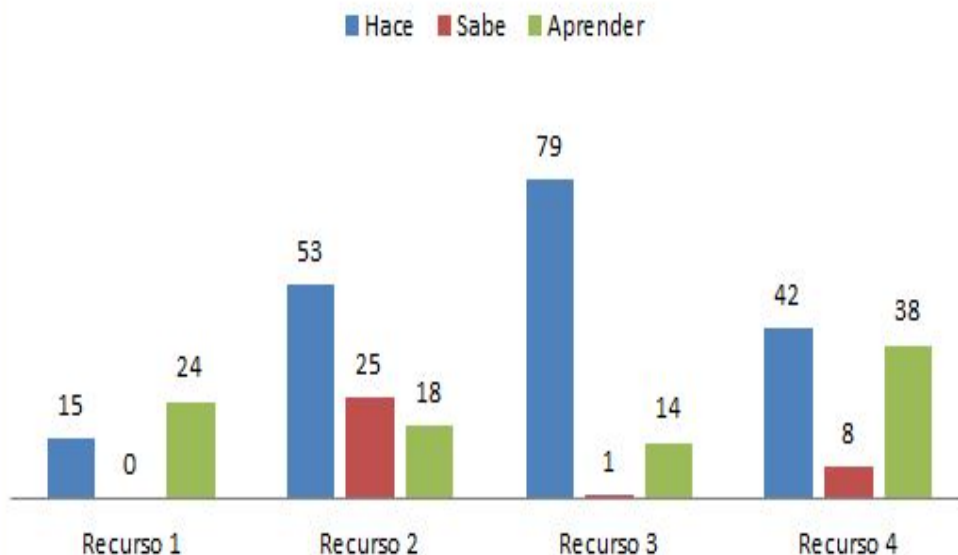
#	Aplic.	Grupo	Tarea	Técnica / Funcional
1	No	Acceso al CPD	Actualización logs en Tablero de Control	Técnica
2	No	Acceso al CPD	Administración de usuarios (ABM)	Técnica
3	No	Acceso al CPD	Configuración del Equipo	Técnica
12	No	Active Directory	Definición de políticas (GPO)	Funcional
13	No	Active Directory	Delegación de Funciones	Técnica
17	No	Administración de claves	Administración de claves de usuarios especiales y de	Funcional
20	No	Análisis de vulnerabilidades	Análisis periódicos de vulnerabilidades en servidores	Técnica
21	No	Análisis de vulnerabilidades	Control sobre administradores locales de las maquinas	Funcional
36	Si	Windows	Administración de usuarios (ABM)	Técnica
37	Si	Windows	Blanqueo de contraseñas	Técnica
38	Si	Windows	Desbloqueo de usuarios	Técnica
40	Si	Windows	Administración de usuarios (ABM)	Técnica
41	Si	Windows	Blanqueo de contraseñas	Técnica
42	Si	Windows	Desbloqueo de usuarios	Técnica
43	No	Auditoria	Atención a Auditores externos e internos (temas Seguridad)	Funcional
44	No	Auditoria	Recolección de información y coordinación de reuniones para responder los informes	Funcional
45	No	Auditoria	Respuesta a Informes de Auditoria	Funcional

Cómo armar e Implementar un PESI?

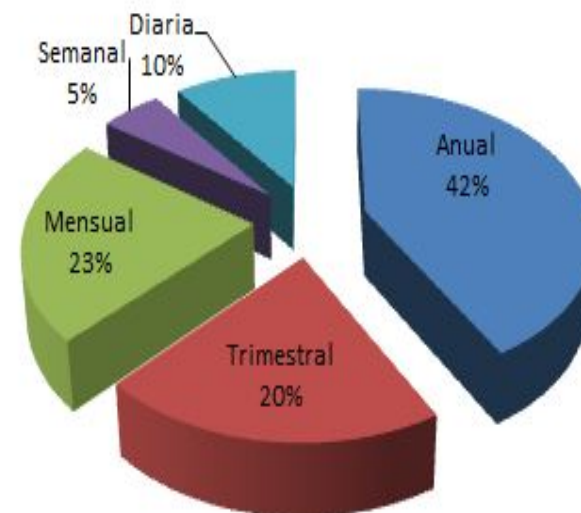
Recurso	Hace	Sabe	Aprender	Total
Recurso 1	15	0	24	39
Recurso 2	53	25	18	96
Recurso 3	79	1	14	94
Recurso 4	42	8	38	88

Frecuencia	Cantidad
Anual	41
Trimestral	20
Mensual	22
Semanal	5
Diaria	10

Distribución de tareas por persona



Distribución de tareas por frecuencia





Cómo armar e Implementar un PESI? (cont.)

Segunda Etapa: Identificar Objetivos

1. Identificar tareas requeridas por normativa determinada.
2. Identificar tareas resultado de procesos controles y/o auditorias previas.
3. Identificar tareas objeto de procesos ajenos a Seguridad de la Información.
4. Identificar los niveles de implementación requeridos por el negocio para cada tarea.
5. Proyectar/Identificar necesidades POST implementación de una tarea.



Cómo armar e Implementar un PESI?

Segunda Etapa: Identificar Objetivos

#	Tareas del Administrador de Seguridad	Año Actual	Prioridad	Año Objetivo (Por ej. 2013)
T	Análisis de Riesgo de TI			
2	Generación de Marco Normativo relacionado al Análisis de Riesgo de TI	L1		L3
3	Planificación para la ejecución del Análisis de Riesgo de TI	L1		L2
4	Implementación del Análisis de Riesgo de TI	L1		L3
5	Comunicación de resultados a las autoridades pertinentes	L1		L2
6	Generación de Plan de Acción en Base a resultados del Análisis de Riesgo de TI y concenso con autoridades pertinentes	L1		L2
T	Desarrollo, mantenimiento e implementación del Marco Normativo de Seguridad de la Información			
8	Generación y publicación de Política de Seguridad (Firmada por la Dirección)	L4		L4
9	Generación y publicación de Normas y procedimientos relacionados a la seguridad de la información	L3		L4
10	Generación y publicación de Procedimientos Operativos (Backup, operación de aplicativos, etc)	L2		L3
11	Generación y publicación de Manual de Misiones y Funciones del Área de Seguridad Informática	L3		L4
12	Generación y publicación de Responsabilidades en Materia de Seguridad de la Información	L3		L4
13	Definición de responsable de establecer contacto con autoridades pertinentes (bomberos, policías, emergencias médicas)	N/A		N/A
14	Revisión de Marco Normativo	L1		L3
T	Foro de Seguridad de la Información			
16	Creación del Foro de Seguridad de la Información	L0		L0
17	Coordinación de reuniones del Foro de Seguridad de la Información	L0		L0



Cómo armar e Implementar un PESI? (cont.)

Tercera Etapa: Armado del PESI

1. Identificar los tiempos requeridos por cada tarea.
2. Identificar responsables de llevarla a cabo / su implementación.
3. Identificar los costos/recursos asociados.
4. Generar el Plan de Implementación y requerimientos externos.





Cómo armar e Implementar un PESI? (cont.)

Cuarta Etapa: Implementación Exitosa

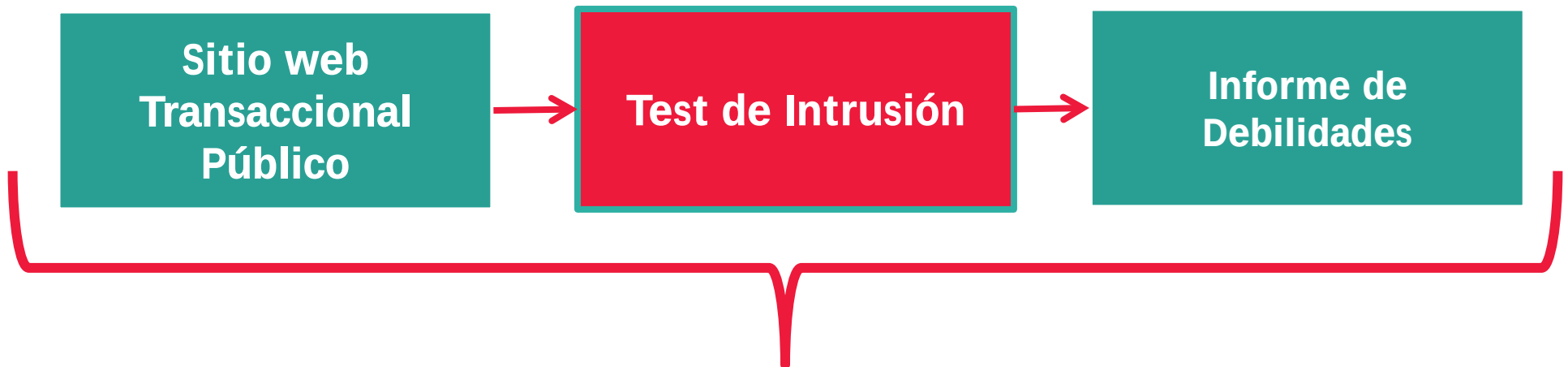
1. Sponsoreo de la Alta Dirección
2. Monitoreo de los avances.
3. Gestión de los retrasos/desvíos.
4. Adecuaciones oportunas.

¡¡ SEGUIMIENTO CONTINUO !!



EJEMPLOS DE NUESTROS SERVICIOS - CONSULTORÍA

Servicio Test de Intrusión



Seguridad en las operaciones de clientes (impacto en la imagen)/empleados.

¿CÓMO PODEMOS AYUDARLO? (cont.)

NORMAS Y REGULACIONES LOCALES E INTERNACIONALES

Diagnóstico, asesoramiento y consultoría para el cumplimiento de diferentes regulaciones y normativas, incluyendo entre las principales: Secc. 404 de la Ley Sarbanes-Oxley, PCI-DSS, SSAE 16 (reemplaza SAS 70), ISAE 3402, ISO 20000, ISO 27000 y otras.



EJEMPLOS DE NUESTROS SERVICIOS - CONSULTORÍA

Servicio PCI-DSS

Validar tarjetas con
Sistema Propio

Diagnóstico PCI-DSS

Presentación a
VISA/Mastercard y
Autorización para
nuevo proceso

Ahorro Económico (menos Postnets y
procesos administrativos eficaces)



PCI - DSS

PREPARADOS PARA EL CAMBIO

El nuevo estándar de la Industria de Tarjetas de Pago se encuentra vigente desde enero de 2014 y será exigible desde enero de 2015.

En BDO pensamos como asistir a nuestros clientes en los nuevos desafíos, por ello desarrollamos metodologías y buenas prácticas para acompañarlos en el cambio.



INFRAESTRUCTURA Y TECNOLOGÍA

Consultoría para áreas de tecnología abarcando implementación, soporte, migración y mantenimiento de sistemas operativos y redes, soluciones seguras de mensajería y correo electrónico, implementación de productos de seguridad informática (herramientas para administración de logs, IDS/IPS), reingeniería de comunicaciones, virtualización de servidores, cloud computing.

SEGURIDAD EN ERP

Diagnóstico y consultoría para evaluar aspectos clave que hacen a la seguridad del sistema, destacando segregación funcional y controles por oposición, roles y funciones, logs de auditoría, accesos de personal del área de TI a funciones de negocio y políticas de seguridad en el aplicativo, bases de datos y sistema operativo.

EJEMPLOS DE NUESTROS SERVICIOS - TERCERIZACIÓN

Servicio Soporte en Infraestructura



**Menos interrupciones del negocio por
indisponibilidad de sistemas.**

NUESTROS ANTECEDENTES

Las principales compañías financieras y bancos de la República Argentina han contratado nuestros servicios, al igual que empresas especializadas en mercados verticales tales como petróleo, telecomunicaciones, datacenters, laboratorios, salud.



NUESTROS ANTECEDENTES



Somos Centro de
Excelencia de LATAM.

¡MUCHAS GRACIAS!

Ing. Pablo Silberfich

Socio

Aseguramiento de Procesos Informáticos

Maipú 942 1° piso

Rondeau 1664, PB

Buenos Aires, Argentina

Tel.: 54 11 4106 7000

Fax: 54 11 4106 7255

www.bdoargentina.com