ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada (MSIA)

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CALIDAD DE LA ISO 27001:2005, PARA APLICAR CONTROLES A LOS ACTIVOS DE UNA ORGANIZACIÓN"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

DALIA YASMIN ORTIZ REINOSO

GUAYAQUIL - ECUADOR

AÑO: 2015

AGRADECIMIENTO

El presente trabajo primeramente me gustaría agradecer a Dios por sus bendiciones, y ser mí guía permanente. A mis padres, mi esposo y hermanos. Sin olvidar a mis compañeros de clases y profesores de MSIA por compartir sus experiencias en los diferentes proyectos realizados que ha sido de aporte fundamental para culminar esta tesis.

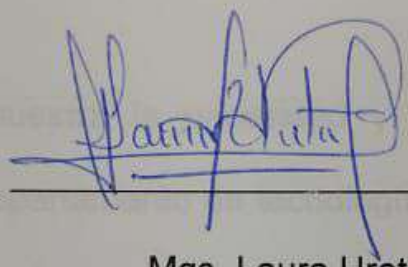
DEDICATORIA

Este logro se lo debo a mi Madre, aunque no está presente en este mundo terrenal me está apoyando a seguir adelante, ella siempre fue mi fortaleza ante las adversidades, supo encaminarme en ser mejor y a cree que nada es imposible si hacemos las cosas de manera honesta y con amor. ¡Gracias Judith! Por los momentos felices, porque fuiste una madre abnegada y amorosa.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR MSIA



Mgs. Laura Ureta

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

Mgs. Albert Espinal

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

RESUMEN

Esta tesis tiene como objetivo implementar el Sistema de Gestión de Calidad de la ISO 27001:2005 en el área de tecnología, manejando procedimientos y controles que ayuda a contrarrestar el mal uso de la información de la organización.

En el capítulo 1 muestra la necesidad y carencia de seguridad de la información de un departamento de tecnología, cuando una institución crece también aumenta los riesgos, los problemas son identificados rápidamente pero la solución no siempre es la más acertada, aplicar los alineamientos de la ISO 27001:2005 nos ayudará contrarrestar los riesgos.

En el capítulo 2 se identifica los activos más importantes de la organización, estos están asignados a grupos según la sensibilidad, origen y valor. Estos activos son valorados según los componentes (Confidencialidad, integridad y disponibilidad), se analiza el riesgo basado en la fórmula probabilidad X impacto, se da el correspondiente tratamiento basados en los controles de la norma ANEXO A ISO 27001:2005 y se crea procedimiento eficiente para los proceso claves.

En el Capitulo 3 muestra los resultados basados en la medición de los datos, previamente son recopilados y por medio de indicadores de resultados podemos medir. Cada proceso es analizado y evaluado, se crea ficha de proceso que nos ayuda identificar con claridad sus entradas y salidas de información, depende mucho de los recursos que se use para que sea la salida esperada.

En este capítulo se demuestra la eficiencia o mal manejo de los controles. El análisis de los indicadores nos permitirá decidir si se corrige o mejora el proceso.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En esta tesis se pretende mejorar los alineamientos internos de los procesos del Departamento de Sistemas, usando técnicas internacionales del estándar ISO 27001:2005.

El Departamento de Tecnología es el área más recurrida para dar y cumplir soluciones día a día, son los responsables de resguardar los activos de la información de la organización, desde ahí partimos en definir los procesos internos o crear procesos que sea de apoyo para proteger la confidencialidad, integridad y disponibilidad de la información.

Se aplica el modelo de Sistema de Gestión de Seguridad de Información Plan-Do-Check-Act (PDCA ó ciclo de Deming) para todos los procesos de la organización. Se implementan los controles para los activos que hemos agrupados (datos, aplicaciones, personal, servicios, tecnología y infraestructura).

La solución propuesta reducirá riesgo operativo mientras que las amenazas son mitigadas. A estos riesgos se aplican tratamientos para minimizar, transferir o controlar según indica la norma [3].

CAPÍTULO 1

GENERALIDADES

1.1 Objetivo General

Aplicar el Sistema de Gestión de Calidad de Seguridad de la Información utilizando la norma ISO-27001:2005, dirigida a una organización cuyo objetivo es brindar un mejor manejo de los activos de la organización.

1.2 Descripción del problema

La ausencia de las buenas prácticas de controles para el manejo de procesos de control de los activos de una organización dentro del departamento de tecnología de una organización, tiende a ser el punto de atracción de los hackers o usuarios mal intencionados, que aprovecha de las vulnerabilidades internas como externas para obtener información valiosa de la organización.

La tesis está direccionada a la administración de un departamento de tecnología que no tiene documentado ningún proceso, procedimiento y política interna de seguridades que ayude a tener los alineamientos correctos para dar control de los activos de la información.

El Dpto. de Tecnología ofrece servicios técnicos a los diferentes programas tales como:

Software operativo.

Software administrativo.

Servicios remotos y locales a usuarios.

Compra de activos.

Mantenimiento de equipos informáticos.

Entre otros.

La administración del departamento de tecnología, actualmente se quiere mejorar los servicios a usuarios finales. A través de ésta tesis se reforzará con los controles internos/externo que ofrece la gestión de calidad.

En la actualidad la dirección de IT NO tiene:

a) Políticas, procedimientos internos de los procesos de IT.
b) Documentación técnica que facilite la asistencia a problemas.
c) No tiene un sistema de inventarios.

d) Equipos informáticos no están asegurados.
e) Control de la información compartida.
f) Seguridad local de equipos computacionales.
g) Control de acceso de usuarios externos.
h) Documentación de incidente de equipo u otros que ayudaría en el control de las emergencias.
i) No existe control de traspaso de equipos informáticos de una sucursal a otra.

Una vez identificados los problemas, es factible identificar los siguientes inconvenientes:

- El empleado tiene acceso a sitios inadecuados que están fuera del contexto laboral.
- No hay registros del servicio a los equipos informáticos a los usuarios.
- No hay registro de mantenimiento de equipos informáticos.
- Tener un repositorio de los incidentes de daño de equipos informáticos.
- Protección eléctrica de los equipos informáticos.

1.3 Solución propuesta

Se debe analizar los procesos del departamento de IT para crear procedimientos y aplicar políticas de seguridad de acuerdo a la norma ISO 27001:2005; poder controlar los accesos internos / externos de la información de la organización, buscar vulnerabilidades que afectarán a la integridad, confiabilidad y la disponibilidad de los datos.

Monitorear y aplicar mejoras continúas en los procesos de la institución a través de los resultados de los indicadores de rendimientos que permiten conocer que procedimientos se están cumpliendo o deben mejorarse.

En la figura 1.1, muestra los controles que hemos identificado como sustanciales para que la implementación tenga éxito y perdure en la administración en el área de Tecnología.

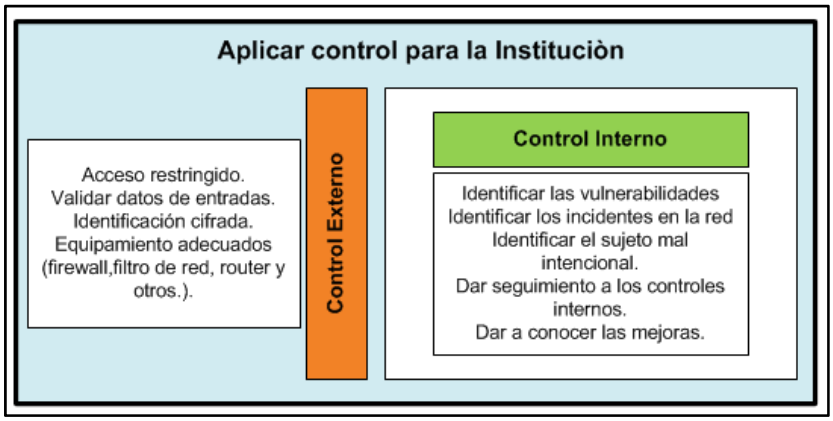


Figura 1.1 Controles para la institución.

Los beneficios son:

1. Control de préstamos o traspaso de equipos informáticos.
2. Confiar en la información obtenida de los sistemas informáticos.
3. Dar un servicio de calidad a usuarios finales.
4. Tener equipos y accesorios informáticos de alta calidad y garantías por parte de proveedores comprometidos.
5. Identificar con facilidad activos que no cumplan con las políticas de tecnología.
6. Control interno del departamento de Tecnología, conocer los registros diarios de eventos o servicios de los activos.

CAPÍTULO 2

ANÁLISIS Y DISEÑO DEL SISTEMAS DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN

2.1 Análisis de los activos

Lo primero que debemos hacer es identificar los activos de la información, este debe diferenciarse por tener características comunes y que la información que almacena o procese tenga el mismo nivel de confidencialidad, integridad o disponibilidad. Vamos crear grupos de aquellos recursos que más adelante vamos aplicar los mismos controles y políticas de seguridad. Cada grupo identificado se debe analizar en que repercuta o impacte en el negocio, y deben ser protegidos.

Revisando el primer capítulo podemos precalificar los grupos de activos más importantes que se presta a dar servicio o son usados de apoyo para obtener la información.

Estos grupos son:

Tabla 1. Crear grupos de activos de la información.

GRUPOS DE ACTIVOS	
Datos:	Manuales de equipos informáticos.
	Manuales de software.
	Disco magnéticos de información.
	Código fuente de aplicativos.
	Informe.
	Contrato.
Aplicaciones:	Sistema financiero.
	Sistema operativo de los equipos.
	Antivirus.
	Base de datos.
Personal:	Usuarios.
	Proveedor.
	Personal general.
	Personal contratado.
Servicios:	Servicio de internet.
	Correo electrónico.
	Autenticación de usuario.

	Administración de proceso de usuario.
	Servicio de red.
Tecnología:	Computador / Laptop.
	Servidor.
	Ruteador / switch / modem.
	Cable de red/cableado.
	Impresora.
	Access point.
Instalaciones / Infraestructura:	Sala de servidores.
	Sala de trabajo.
	Archivadores.

Inventariar los activos que realice una gestión ante algún desastre, recuerde que debe identificarse activos que sean relevante para el negocio [1]. Vamos ponerlo en un formato:

Tabla 2. Identificar los activos de la información.

IDENTIFICAR LOS ACTIVOS				
Código	**Grupo**	**Descripción**	**Propietario**	**Ubicación**
001	Datos	Manuales instructivo de equipos y aplicativos.	Jefe de sistema	Dpto. Sistemas

002	Datos	Contratos.	Jefe de sistema	Dpto. Sistemas
003	Datos	Medio de almacenamiento (disco magnético)	Técnico	Dpto. Sistemas
004	Aplicaciones	Sistema financiero	Analista	Dpto. Sistemas
005	Aplicaciones	Sistemas operativos	Técnico	Dpto. Sistemas
006	Aplicaciones	Herramientas aplicativas	Técnico	Dpto. Sistemas
007	Aplicaciones	Antivirus	Técnico	Dpto. Sistemas
008	Aplicaciones	Base de datos.	Analista	Dpto. Sistemas
009	Personal	Proveedor	Terceros	Terceros
010	Personal	Usuarios	Jefe de sistemas	Varios departamentos
011	Servicios	Servicio de internet.	Técnico	Dpto. Sistemas
012	Servicios	Correo electrónico.	Jefe de sistemas	Dpto. Sistemas
013	Servicios	Autenticación de usuario	Jefe de sistemas	Dpto. Sistemas
014	Servicios	Administración de proceso de usuario	Jefe de sistemas	Dpto. Sistemas
015	Servicios	Servicio de red	Técnico	Dpto. Sistemas
016	Tecnología	Computador	Técnico	Dpto. Sistemas
017	Tecnología	Laptop	Técnico	Dpto. Sistemas
018	Tecnología	Servidor	Técnico	Dpto. Sistemas
019	Tecnología	Ruteador / switch	Técnico	Dpto.

				Sistemas
020	Tecnología	Cableado	Técnico	Dpto. Sistemas
021	Instalaciones	Sala de servidores	Técnico	Dpto. Sistemas
022	Instalaciones	Sala de trabajo	Técnico	Dpto. Sistemas

Una vez identificado los activos más importantes, hago uso de varias plantillas que no es más que un documento colaborativo creado por la ISO/IEC 27001/27002, perteneciente a un grupo de personas que implementa estándares de gestión de seguridad de la información [2].

Los activos de información deben ser medidos o tasado para conocer el impacto que causará en la organización. En la tabla 3, va definir los niveles de impacto sobre los componentes (Confidencialidad, integridad y disponibilidad) [2].

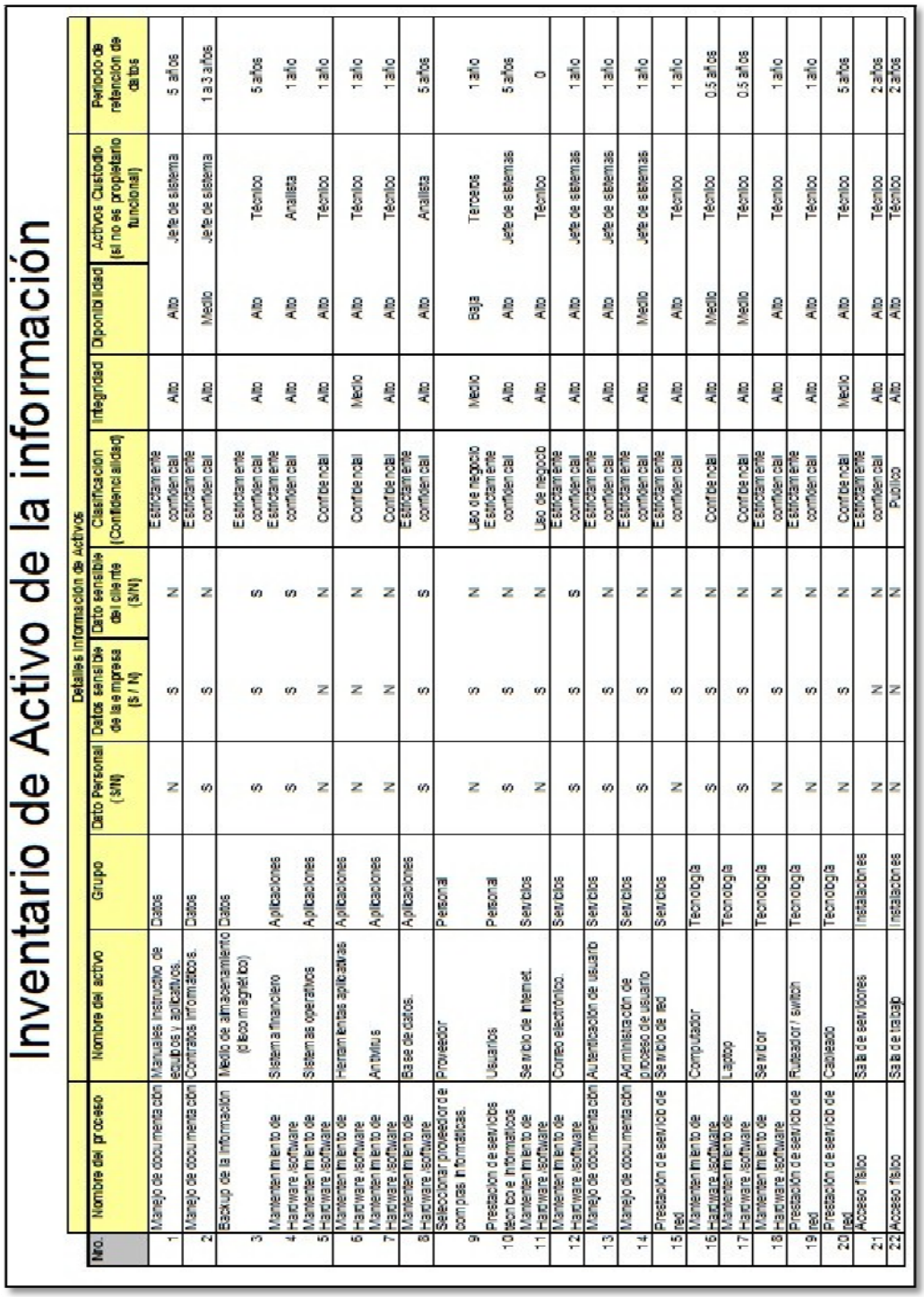
Tabla 3. Definición de nivel de impacto hacia la organización.

Confidencialidad		
Nivel	Definición	Impacto de la protección de la información
Estrictamente confidencial	Muy sensible o privada de la organización, sólo usada por personal autorizado.	Causa daño grave, gastos económicos grandes, pérdida competitiva dentro del mercado.
Confidencial	Sólo personal autorizada, no puede ser divulgado por parte pública o externas.	Causa daño limitado a la organización, pérdida económica mediana.
Uso de negocio	Información permitida por el dueño de la información.	Impacto mínimo, que no afecta a la organización.
Pública	No hay requisito de seguridad.	No hay impacto.
Integridad		
Nivel	Definición	Impacto de la modificación no autorizada
Alto	100% libre de errores.	Igual que la clasificación de confidencialidad de la información estrictamente confidencial.
Medio	96-99% libre de errores.	Igual que la clasificación de confidencialidad de la información confidencial.
Bajo	90-95% libre de errores.	Igual que la clasificación de confidencialidad para negocios utilizan sólo información.
Disponibilidad		
Nivel	Definición	Impacto de la falta de disponibilidad
Alto	No hay interrupción más allá de 0.5 días.	Impacto adverso grave.
Medio	Sin interrupción de acceso más allá de 1 día.	Impacto adverso significativo.

Bajo	Sin interrupción de acceso más allá de 7 días.	Sin interrupción de acceso más allá de 7 días. Impacto adverso limitado.

En la figura 2.1 se detalla lo siguiente:

Muestra los procesos que están involucrados los activos, a qué grupo pertenece, que tan sensible son sus datos, que impacto tendría con los componentes (Confidencialidad, integridad y disponibilidad), quienes son sus custodios, tiempo que prevalece la información de los activos.



Inventario de Activo de la información

Nro.	Nombre del proceso	Detalles información de Activos										Periodo de retención de datos
		Nombre del activo	Grupo	Dato Personal (S/N)	Datos sensible de la empresa (S / N)	Dato sensible del cliente (S/N)	Clasificacion (Confidencialidad)	Integridad	Disponibilidad	Activos Custodio (si no es propietario funcional)	
1	Manejo de documentacion	Manuales instructivo de equipos u aplicativos.	Datos	N	S	N	Estrictamente confidencial	Alto	Alto	Jefe de sistema	5 años
2	Manejo de documentacion	Contratos informaticos.	Datos	S	S	N	Estrictamente confidencial	Alto	Medio	Jefe de sistema	1 a 3 años
3	Backup de la information	Medio de almacenamiento (disco magnetico)	Datos	S	S	S	Estrictamente confidencial	Alto	Alto	Técnico	5 años
4	Mantenimiento de Hardware /software	Sistema financiero	Aplicaciones	S	S	S	Estrictamente confidencial	Alto	Alto	Analista	1 año
5	Mantenimiento de Hardware /software	Sistemas operativos	Aplicaciones	N	N	N	Confidencial	Alto	Alto	Técnico	1 año
6	Mantenimiento de Hardware /software	Herramientas aplicativas	Aplicaciones	N	N	N	Confidencial	Medio	Alto	Técnico	1 año
7	Mantenimiento de Hardware /software	Antivirus	Aplicaciones	N	N	N	Confidencial	Alto	Alto	Técnico	1 año
8	Mantenimiento de Hardware /software	Base de datos.	Aplicaciones	S	S	S	Estrictamente confidencial	Alto	Alto	Analista	5 años
9	Seleccionar proveedor de compras informaticas.	Proveedor	Personal	N	S	N	Uso de negocio	Medio	Baja	Tercero	1 año
10	Prestacion de servicios tecnico e informaticos	Usuarios	Personal	S	S	N	Estrictamente confidencial	Alto	Alto	Jefe de sistemas	5 años
11	Mantenimiento de Hardware /software	Servicio de Internet.	Servicios	N	S	N	Uso de negocio	Alto	Alto	Técnico	0
12	Mantenimiento de Hardware /software	Correo electronico.	Servicios	S	S	S	Estrictamente confidencial	Alto	Alto	Jefe de sistemas	1 año
13	Manejo de documentacion	Autenticacion de usuario	Servicios	S	S	N	Estrictamente confidencial	Alto	Alto	Jefe de sistemas	1 año
14	Manejo de documentacion	Administracion de proceso de usuario	Servicios	S	S	N	Estrictamente confidencial	Alto	Medio	Jefe de sistemas	1 año
15	Prestacion de servicio de red	Servicio de red	Servicios	N	S	N	Estrictamente confidencial	Alto	Alto	Técnico	1 año
16	Mantenimiento de Hardware /software	Computador	Tecnologia	S	S	N	Confidencial	Alto	Medio	Técnico	0.5 años
17	Mantenimiento de Hardware /software	Laptop	Tecnologia	S	S	N	Confidencial	Alto	Medio	Técnico	0.5 años
18	Mantenimiento de Hardware /software	Servidor	Tecnologia	N	S	N	Estrictamente confidencial	Alto	Alto	Técnico	1 año
19	Prestacion de servicio de red	Ruteador / switch	Tecnologia	N	S	N	Estrictamente confidencial	Alto	Alto	Técnico	1 año
20	Prestacion de servicio de red	Cableado	Tecnologia	N	S	N	Confidencial	Medio	Alto	Técnico	5 años
21	Acceso fisico	Sala de servidores	Instalaciones	N	N	N	Estrictamente confidencial	Alto	Alto	Técnico	2 años
22	Acceso fisico	Sala de trabajo	Instalaciones	N	N	N	Publico	Alto	Alto	Técnico	2 años

Figura 2.1 Documento de inventario de activo y la valoración de la información de la organización.

2.2 Análisis de gestión de riesgo

Definidos los activos de la información con sus procesos, ahora se mide o valora al riesgo basado en la metodología del estándar internacional ISO/IEC 27001:2005 [3], estamos haciendo uso de plantilla [2] que nos ayudará identificar el valor porcentual del impacto y la probabilidad que se dé el riesgo dentro de la organización. A continuación la figura 2.2, es tomada de referencia para aplicar los criterios para el análisis de los riesgos, como se muestra en la figura 2.3.

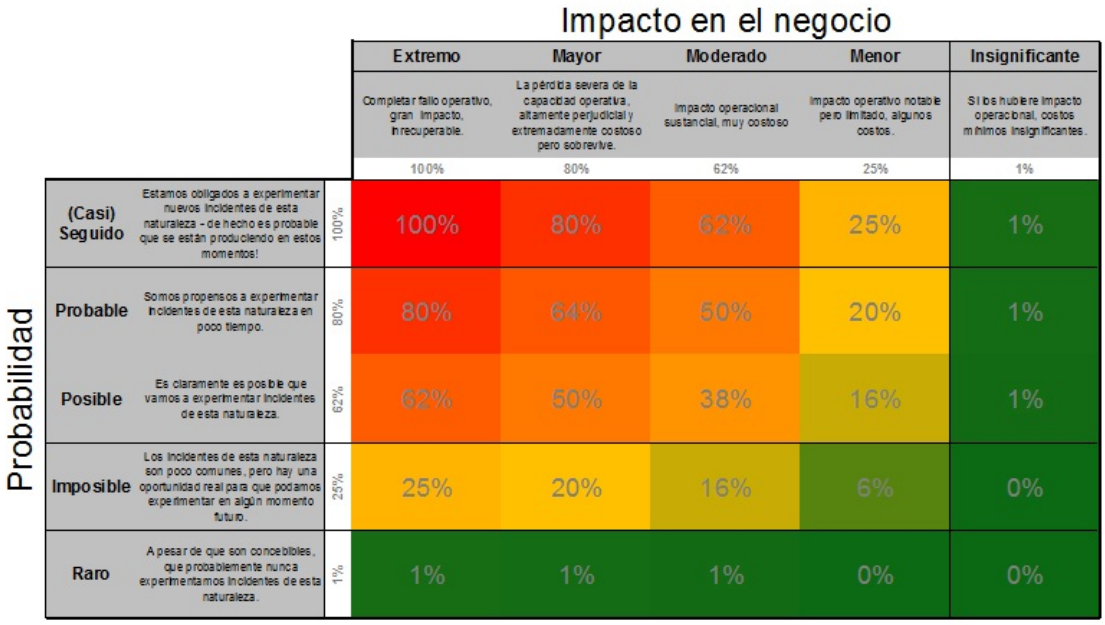
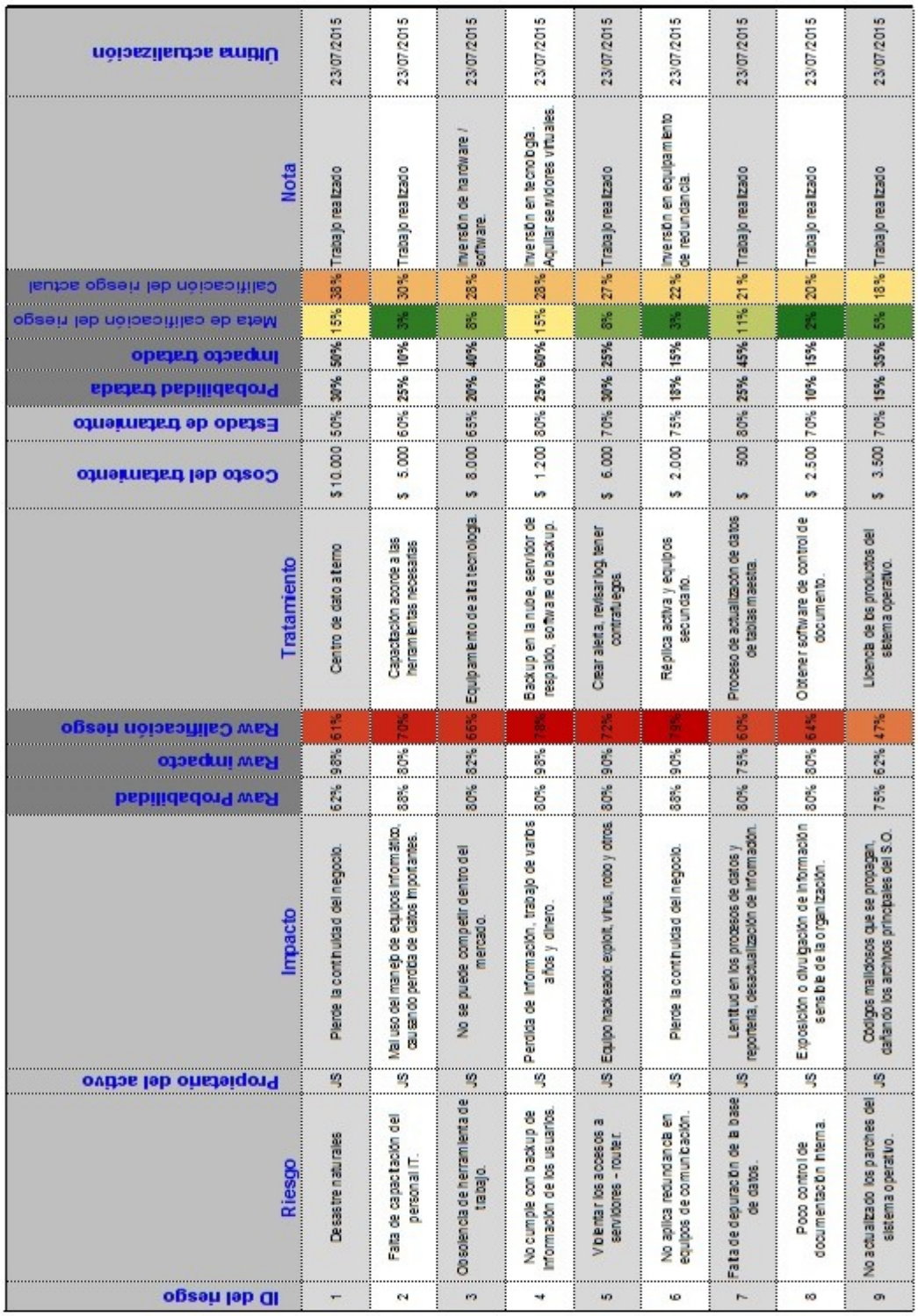
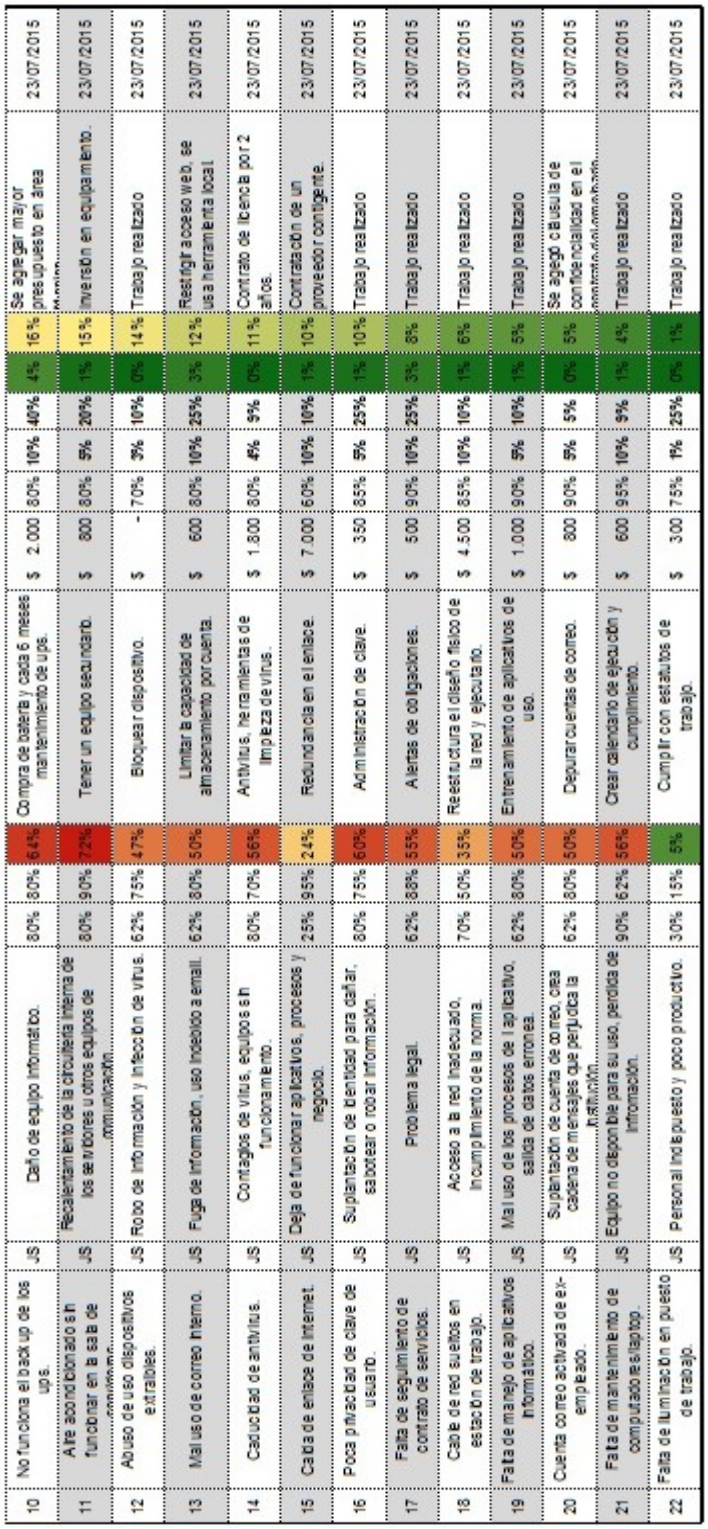


Figura 2.2 Evaluación porcentual de Riesgo = Probabilidad x Impacto [2].



ID del riesgo	Riesgo	Propietario del activo	Impacto	Raw Probabilidad	Raw Impacto	Raw Calificación riesgo	Tratamiento	Costo del tratamiento	Estado de tratamiento	Probabilidad tratada	Impacto tratado	Meta de calificación del riesgo	Calificación del riesgo actual	Nota	Última actualización
1	Desastre naturales	JS	Pierde la continuidad del negocio.	62%	98%	61%	Centro de dato alterno	$ 10.000	50%	30%	50%	15%	38%	Trabajo realizado	23/07/2015
2	Falta de capacitación del personal IT.	JS	Mal uso del manejo de equipos informático, causando perdida de datos importantes.	88%	80%	70%	Capacitación acorde a las herramientas necesitas	$ 5.000	60%	25%	10%	3%	30%	Trabajo realizado	23/07/2015
3	Obsolencia de herramienta de trabajo.	JS	No se puede competir dentro del mercado.	80%	82%	66%	Equipamiento de alta tecnologia.	$ 8.000	65%	20%	40%	8%	28%	Inversión de hardware / software.	23/07/2015
4	No cumple con backup de información de los usuarios.	JS	Perdida de información, trabajo de varios años y dinero.	80%	98%	78%	Backup en la nube, servidor de respaldo, software de backup.	$ 1.200	80%	25%	60%	15%	28%	Inversión en tecnologia. Aquilar servidores virtuales.	23/07/2015
5	Violentar los accesos a servidores - router.	JS	Equipo hackeado exploit, virus, robo y otros.	80%	90%	72%	Crear alerta, revisar log, tener contratiempo.	$ 6.000	70%	30%	25%	8%	27%	Trabajo realizado	23/07/2015
6	No aplica redundancia en equipos de comunicación.	JS	Pierde la continuidad del negocio.	88%	90%	79%	Réplica activa y equipos secundario.	$ 2.000	75%	18%	15%	3%	22%	Inversión en equipamiento de redundancia.	23/07/2015
7	Falta de depuración de la base de datos.	JS	Lentitud en los procesos de datos y reportería, desactualización de información.	80%	75%	60%	Proceso de actualización de datos de tablas maestra.	$ 500	80%	25%	45%	11%	21%	Trabajo realizado	23/07/2015
8	Poco control de documentación interna.	JS	Exposición o divulgación de información sensible de la organización.	80%	80%	64%	Obtener software de control de documento.	$ 2.500	70%	10%	15%	2%	20%	Trabajo realizado	23/07/2015
9	No actualizado los parches del sistema operativo.	JS	Códigos malicioso que se propagan, dañando los archivos principales del S.O.	75%	82%	47%	Licencia de los productos del sistema operativo.	$ 3.500	70%	15%	35%	5%	18%	Trabajo realizado	23/07/2015

Figura 2.3. Análisis y evaluación del riesgo.



10	No funciona el back up de los ups.	JS	Daño de equipo Informático.	80%	80%	64%	Compra de batería y cada 6 meses mantenimiento de ups.	$	2.000	80%	10%	40%	4%	16%	Se agregar mayor presupuesto en área		23/07/2015
11	Aire acondicionado sin funcionar en la sala de	JS	Recalentamiento de la circuitería interna de los servidores u otros equipos de	80%	90%	72%	Tener un equipo secundario.	$	800	80%	5%	20%	1%	15%	Inversión en equipamiento.		23/07/2015
12	Abuso de uso dispositivos extraibles.	JS	Robo de información y infección de virus.	62%	75%	47%	Bloquear dispositivo.	$	-	70%	3%	10%	0%	14%	Trabajo realizado		23/07/2015
13	Mal uso de correo interno.	JS	Fuga de información, uso indebido a email.	62%	80%	50%	Limitar la capacidad de almacenamiento por cuenta.	$	600	80%	10%	25%	3%	12%	Restigir acceso web, se usa herramienta local		23/07/2015
14	Caducidad de antivirus.	JS	Contagios de virus, equipos sin funcionamiento	80%	70%	56%	Antivirus, herramientas de limpieza de virus.	$	1.800	80%	4%	9%	0%	11%	Contrato de licencia por 2 años.		23/07/2015
15	Caida de enlace de internet.	JS	Deja de funcionar aplicativos, procesos y negocio.	25%	95%	24%	Redundancia en el enlace.	$	7.000	60%	10%	10%	1%	10%	Contratación de un proveedor contigente.		23/07/2015
16	Poca privacidad de clave de usuario.	JS	Suplantación de identidad para dañar, sabotear o robar información.	80%	75%	60%	Administración de clave.	$	350	85%	5%	25%	1%	10%	Trabajo realizado		23/07/2015
17	Falta de seguimiento de contrato de servicios.	JS	Problema legal.	62%	88%	55%	Alertas de obligaciones.	$	500	90%	10%	25%	3%	8%	Trabajo realizado		23/07/2015
18	Cable de red sueltos en estación de trabajo	JS	Acceso a la red inadecuado, incumplimiento de la norma	70%	50%	35%	Reestructura el diseño físico de la red y ejecutarlo	$	4.500	85%	10%	10%	1%	6%	Trabajo realizado		23/07/2015
19	Falta de manejo de aplicativos informático.	JS	Mal uso de los procesos de l aplicativo, salida de datos erroneo.	62%	80%	50%	Entrenamiento de aplicativos de uso.	$	1.000	90%	5%	10%	1%	5%	Trabajo realizado		23/07/2015
20	Cuenta correo activada de ex-empleado.	JS	Suplantación de cuenta de correo, crea cadena de mensajes que perjudica la	62%	80%	50%	Depurar cuentas de correo.	$	800	90%	5%	5%	0%	5%	Se agrego cláusula de confidencialidad en el		23/07/2015
21	Falta de mantenimiento de computadores/laptop.	JS	Equipo no disponible para su uso, perdida de información.	90%	62%	56%	Crear calendario de ejecución y cumplimiento.	$	600	95%	10%	9%	1%	4%	Trabajo realizado		23/07/2015
22	Falta de iluminación en puesto de trabajo.	JS	Personal indispuesto y poco productivo.	30%	15%	5%	Cumplir con estatutos de trabajo.	$	300	75%	1%	25%	0%	1%	Trabajo realizado		23/07/2015

Figura 2.4 Continuación del análisis y evaluación del riesgo.

Ahora, vamos aplicar objetivo de control y controles del ANEXO A del estándar internacional ISO/IEC 27001:2005 [3] basándose de los resultados del análisis y evaluación del riesgo, para cumplir con la meta y hacer funcionar el **tratamiento** indicado del documento (Figura 2.3 y 2.4).

Estos controles serán aplicados en el tratamiento de los riesgos.

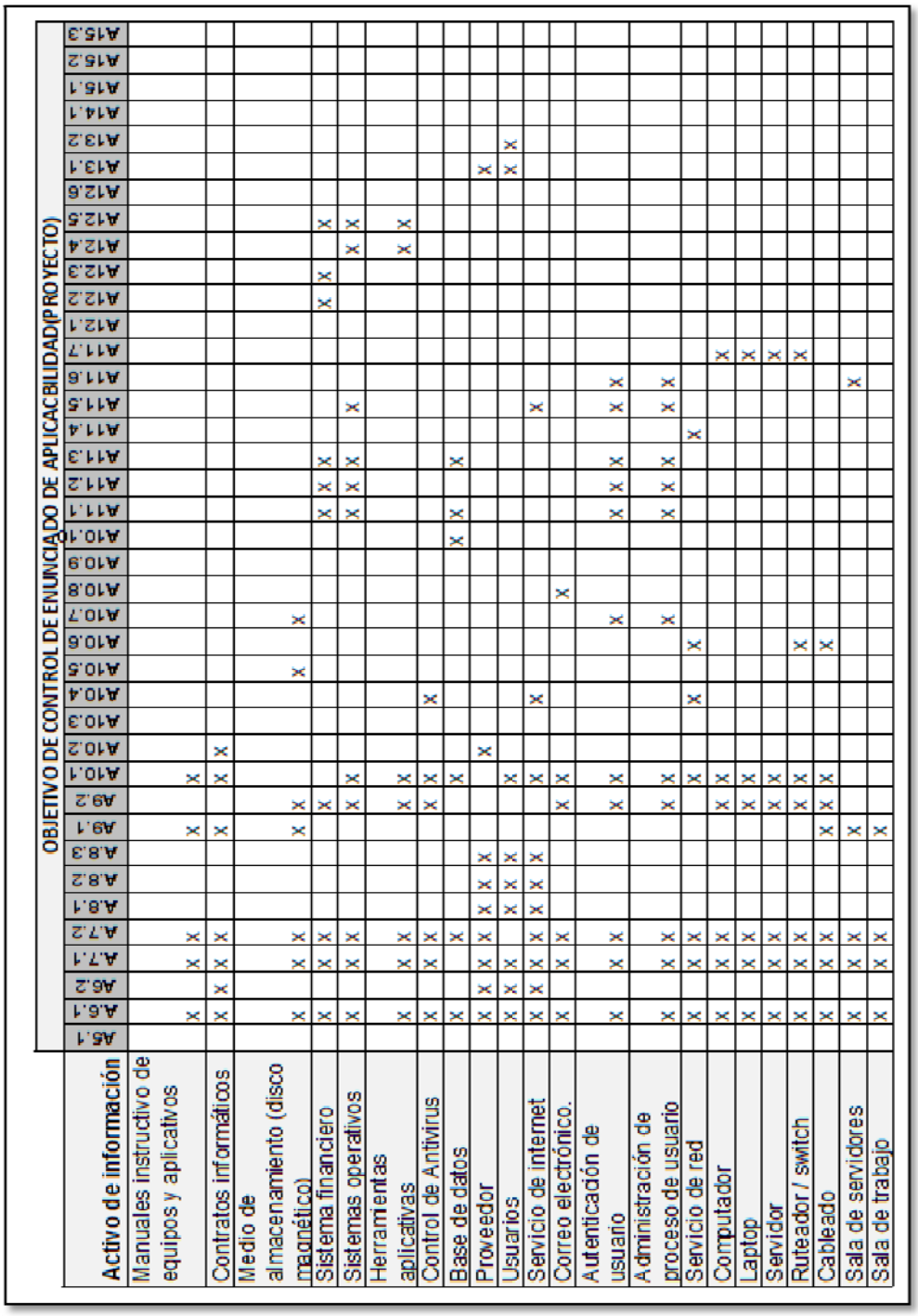


Figura 2.5 Planteamiento del enunciado de aplicabilidad.

2.3 Análisis de los proceso internos

Todo servicio que ofrece el departamento de tecnología se deriva en múltiples tareas, de aquí se crea los procesos, estos se diferencian en principales y secundarios.

Considero los procesos principales aquellos que son claves para que se ejecute el servicio.

Identifiquemos los procesos internos que están en el documento de inventario de activo y la valoración de la información de la organización, fíjese en la figura 2.1, a continuación se detalla:

- Manejo de documentación.
- Backup de la información.
- Mantenimiento de hardware / software.
- Seleccionar proveedor de compras informáticas.
- Prestación de servicio de red.
- Acceso físico.
- Prestación de servicio de red.
- Inventario de hardware / software.
- Acceso físico al cuarto de servidores.
- Control de acceso de software informático.
- Manejo de contrato y documentación interna IT.

2.4. Crear Mapa de procesos

Identificado los procesos, se crea un diseño basado en los servicios que se da al usuario, se mide los resultados para conocer que procesos son los más importantes y otros que son de apoyo. Que procesos son los que cumple con lo que requiere la organización, se puede conocer de donde viene, su realización y quién lo hizo. Observe la figura 2.6.

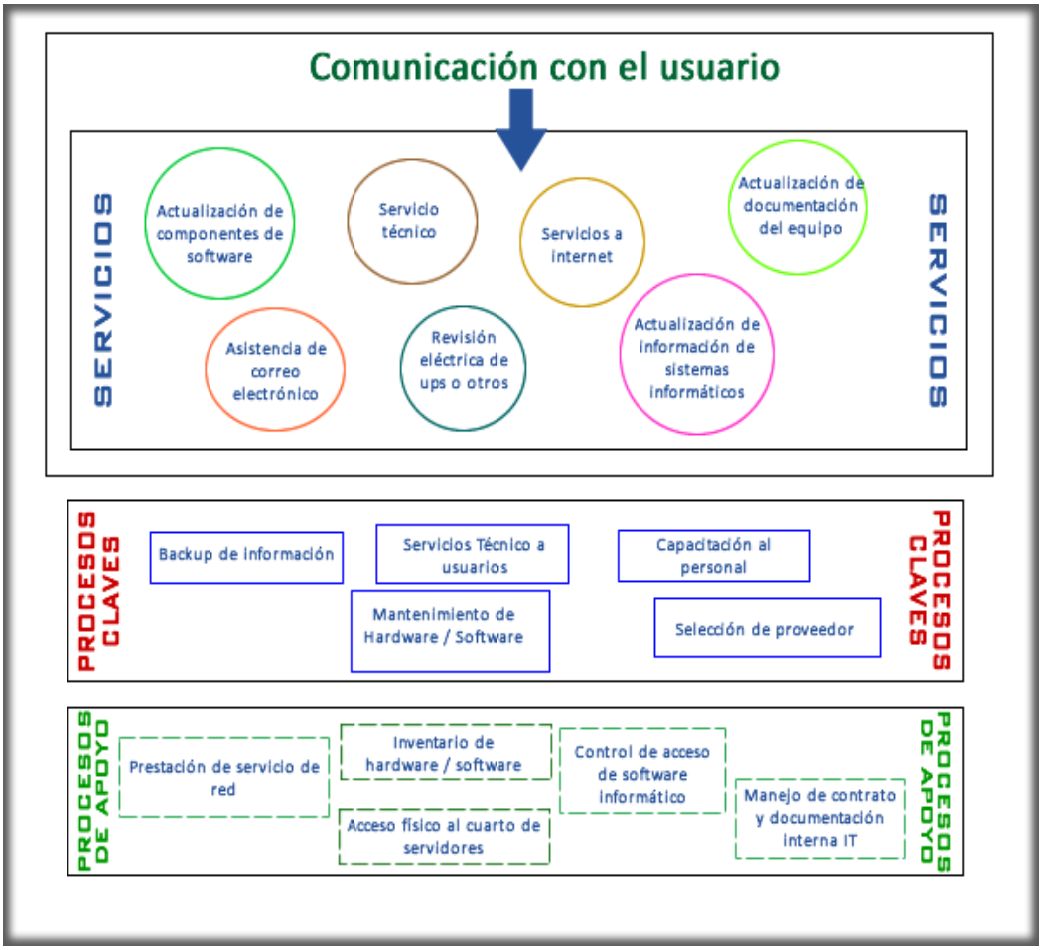


Figura 2.6 Mapa de procesos

2.5 Diseñar controles usando alineamiento de seguridad que indica la norma ISO-2700.

Se crea los alineamientos para los controles escogida, obsérvese en la Figura 2.5.

Cada control está basado en el ANEXO A del estándar internacional ISO/IEC 27001:2005 [3].

Control

La asignación de las responsabilidades de seguridad de la información

Alineamientos: La personas involucradas en cada proceso, debe estar capacitada, dispuesta a cumplir y a hacer cumplir cada disposición que la norma indique.

- El responsable debe estar plenamente capacitado para seguir con los objetivos.
- Debe ser capaz de reconocer cuando un control no funciona o debe ser cambiado.
- Debe mostrar los resultados mediantes indicadores.

Control:

La responsabilidad de los activos y su clasificación de la información.

Alineamientos:

- Cada activo debe estar plenamente identificado y clasificado en función de su valor, requisitos legales, sensibilidad y criticidad.
- Inventariar los activos y dejar ubicado donde corresponda, conocer el custodio del activo.
- Tener equipos en buen estado y bien configurado.
- Crear normas de control para el uso del activo, y difundirlo a los usuarios.

Control:

La seguridad de los recursos humanos antes, durante y después de su contratación.

Alineamientos:

- Debe conocer sus funciones y responsabilidades del puesto de trabajo, no sólo al empleado, también el personal contratista.
- Dentro del contrato debe adaptarse cláusula de responsabilidad de los activos que se le asigne.
- Debe existir controles de verificación del antecedente del candidato, para que cumpla con el perfil.

- Debe crearse políticas de concienciación para evitar fraude, robo y modificaciones con los activos de la información.
- La desvinculación del empleado debe asegurar que entregue los activos que fueron dados al inicio de su contratación.
- Se debe eliminar todo tipo de documentos o registros que vincule al ex - empleado.

Control:

Evitar el acceso no autorizado físico, perjuicio e interferencia en las instalaciones y a la información de la institución.

Alineamientos:

- El área de trabajo donde se encuentre la información de la organización debería estar protegido con seguridades, usando controles biométricos o tarjetas magnéticas, en especial el cuarto de servidores.
- Debe existir un manual o proceso en caso de desastre, donde permita levantar los procesos más importantes para la continuidad del negocio.
- La ubicación física donde repose los backup de la información debe estar aseguradas con controles electrónicos y fuera de la vista de los usuarios no autorizados.

- Todo equipo externo que ingrese a las instalaciones debe ser registrado. Evite fuga de información.
- Mientras se opere el equipo no se debe consumir alimentos ni bebidas que pueda dañar o causar un desastre.
- Suministrar aire acondicionado adecuado en oficina de trabajo, buen funcionamiento eléctrico en tomas de corrientes e iluminaciones, equipo contra incendio, alarma de monitoreo y otros.

Control:

Mantener en buen funcionamiento los equipos informáticos, controlar la fuga de información e interrumpir la disponibilidad de la información.

Alineamientos:

- Mantenimiento semestral de los equipos de cómputos de las estaciones de trabajo, este mantenimiento debe ser preventivo y correctivo.
- Usar aplicativo o software de control de inventario, donde se documente los grupos de activos de la organización y su ubicación física.
- Debe estar protegido con ups.
- Todo daño físico o lógico, debe ser llenado en una bitácora de suceso.

- Debe existir una medición de las incidencias para controlar eventos sospechosos y poder ejecutar los controles adecuados.
- No interrumpir la garantía de los equipos.
- Tener póliza de seguros para los equipos informáticos y de comunicación.
- Restringir el acceso a equipos en lugares públicos.

Control:

Protección contra código malicioso, control de backup de la información y acceso a la red de la organización.

Alineamientos:

- Licenciamiento de antivirus, control de actualización del antivirus.
- Actualización de parches de los sistemas operativos y software de aplicativos.
- Controlar los documentos adjuntos de los correos electrónico, evite el contagio de virus.
- Identificar página web que contenga código maliciosos que se propaguen en su equipo. Notificar al usuario de estos sitios, concientizar al usuario.
- Manejar un cronograma de backup de información, y separarlos en grupos según su sensibilidad.

- El almacenamiento de la información (backup) debe estar fuera y dentro de la institución, puede hacer uso de servidores virtualizado para almacenar información sensible de la organización.
- Todo equipo debe ser identificado en la red, agregar en grupo dependiendo de las tareas de las funciones del empleado.
- Monitorear la red, uso de herramientas para controlar el acceso en la red, permitidos dentro o fuera de la organización, aplicar controles para los eventos e identificar los incidentes en la red. Realice documentaciones de eventos e incidentes para medir sus consecuencias.
- Identificación de equipos remoto, crear restricciones dentro la red.

Control:

Gestión de acceso a usuarios, sus responsabilidades y control de acceso a la red y al sistema operativo de la organización.

Alineamientos:

- Debe existir un registro de creación de contraseña, como también su eliminación.
- Los accesos de cuentas son previlejados y limitados.
- Solo se accede a equipos asignado.

- La contraseña se debe cambiar constantemente para evitar accesos no autorizados.
- El usuario debe seguir las políticas de las buenas prácticas de seguridad de las contraseñas.
- Crear subredes según el tipo servicio que ofrezca, debe existir un control de autenticación y regístrelo.
- Los accesos remotos, debe ser limitado y usar método autenticados.
- El acceso al sistema operativo debe ser seguro, debe usar herramientas capaces y controladas dentro del ambiente.
- La sesión inactiva del sistema operativo debe bloquearse la pantalla, para proteger el acceso a la información.

2.6 Diseñar los procedimientos de los procesos internos de los servicios que ofrece el departamento de tecnología.

Se crea los procedimientos para mejorar los servicios a usuarios, se define los objetivos, alcances, responsables, herramientas y registros, para mejorar de manera eficiente y sistemática las asistencias solicitadas.

Los procedimientos son pasos a seguir para cumplir objetivos, donde se define las responsabilidades, recursos y registros, que permite en entregar un servicio acorde a las metas que tiene la organización.

Procedimientos a seguir:

Servicios técnicos a usuarios.

Mantenimiento Hardware / software y backup de la información.

Capacitación al personal.

Procedimiento: Servicios técnicos a usuarios.

OBJETIVO

Direccionar el método para la realización del Servicio Técnico a cada área de la Institución.

ALCANCE:

Aplica el servicio técnico de hardware/software, equipo de audio y video, incluyendo: Instalación, configuración y poner en marcha el equipo.

RESPONSABLES:

Es responsabilidad del Técnico elaborar y velar por el cumplimiento de este procedimiento.

Es responsabilidad del Director / Gerente la aprobación de este procedimiento.

DESCRIPCIÓN DEL PROCEDIMIENTO

DESCRIPCIÓN DE ACTIVIDADES

Tabla 4 Descripción de actividades del servicios técnicos.

Responsable	Secuencia	Actividad
Solicitante	01	Solicita atención técnica usando la Solicitud de Servicio Técnico (Formato Libre); en la que detalla datos del Solicitante (Nombre, área, la atención requerida y un breve detalle del requerimiento)
Técnico	02	Recepta la Solicitud de Servicio Técnico (Formato Libre) y da la asistencia remota pero en caso de problema físico se dirige al puesto de trabajo.
Técnico	03	En caso de necesitar repuesto o accesorios informático debe solicitar al jefe del área.
Jefe de sistemas	04	Entrega requerimiento usando el Registro de Solicitud – Entrega de Equipos, repuestos, accesorios y Suministros (Formato Libre). En caso de no existir en almacenamiento, solicita compra de materiales usando la Requisición de Asistencia (Formato Administrativo).
Técnico	05	Realizado el trabajo, procede a entregar el equipo operativo, y pone la asistencia atendida en el formato de Solicitud de Servicio Técnico (Formato Libre).

REFERENCIAS:

Catálogos y Manuales de Equipos / dispositivos informáticos.

DEFINICIONES:

N/A

REGISTROS:

Solicitud de Servicio Técnico (Formato Libre)

Registro de Solicitud – Entrega de Equipos, repuestos, accesorios y Suministros (Formato Libre).

Requisición de Asistencia (Formato Administrativo).

Procedimiento: Mantenimiento Hardware / software y backup de la información.

OBJETIVO

Direccionar las actividades para dar mantenimiento preventivo y correctivo a equipos y software informático para mantenerlos en buen estado y operativos para el uso interno de la organización, además almacenar backup de base de datos para tener resguardada la información de la institución.

ALCANCE:

Aplica al proceso de Mantenimiento de Hardware, Software y Backups.

RESPONSABLES:

Es responsabilidad del Administrador de Base de datos y Técnico gestionar el proceso de Mantenimiento de Hardware, Software y Backups, así como el cumplimiento del presente procedimiento. Es responsabilidad del Director / Gerente para la aprobación de este procedimiento.

DESCRIPCIÓN DEL PROCEDIMIENTO

Tabla 5 Descripción de actividades del Mantenimientos varios.

Responsable	Secuencia	Actividad
Técnico	01	***Cumple las actividades del Registro de Control Mantenimiento de Hardware y Software (Formato Libre)***
Administrador de Red	02	***Cumple las actividades del Registro de Control de Backup de Base de Datos (Formato Libre)***
Administrador de Red	03	***Cumple las actividades del Registro de Backup de Información del Usuario (Formato Libre)***
Técnico	04	Entrega el equipo informático sometido a mantenimiento, y en funcionamiento
Técnico	05	En el caso de que el equipo no quede operativo después de someterse al mantenimiento se lo reporta al Jefe Inmediato (Formato Libre)
Jefe de sistemas	06	Reporta equipo en baja a Financiero

REFERENCIAS:

N/A

DEFINICIONES:

N/A

REGISTROS:

Registro de Control Mantenimiento de Hardware y Software (Formato Libre).

Registro de Control de Backup de Base de Datos (Formato Libre).

Registro de Backup de Información del Usuario (Formato Libre).

Procedimiento: Capacitación al personal.

OBJETIVO:

Describir la forma en cómo se planifica y ejecuta el proceso de capacitación de sistemas informáticos y de herramientas al personal de tecnología y usuarios dentro de la Institución con la finalidad de mantener un recurso humano que pueda hacer uso de herramientas de forma adecuada para su normal desarrollo de la Institución.

ALCANCE:

Este procedimiento aplica a la capacitación de colaboradores de IT y usuarios varios.

RESPONSABLES:

Es responsabilidad del Jefe de sistemas gestionar el proceso de capacitación y asegurar el cumplimiento del presente procedimiento.

Es responsabilidad del Director / Gerente aprobar el presente procedimiento.

La responsabilidad en la ejecución y cumplimiento del presente procedimiento involucra a todos los usuarios y colaboradores de IT.

DESCRIPCIÓN DEL PROCEDIMIENTO:

DESCRIPCIÓN DE LAS ACTIVIDADES

Tabla 6 Descripción de actividades de la capacitación.

Responsable	Secuencia	Actividad
Jefe de sistemas	01	Detectar la necesidad de capacitación a personal recién contratado o antiguo. Detectar la necesidad de capacitación del personal a su cargo a su vez realizando un análisis a través del registro de: Documento de Descripción de Funciones.
Jefe de sistemas	02	Elabora/corrige el Plan de Capacitación (Formato libre) en base a la información obtenida de la actividad del punto anterior.
Director / Gerente	03	Revisa y aprueba la capacitación y recursos disponibles, de no estar de acuerdo (regresa al paso anterior).
Jefe de sistema / Director - Gerente	04	Establecen la forma de dar la capacitación requerida para cada curso: interna o externa.
Participante / Jefe de sistemas	05	Para el caso de capacitación No Programada, solicita aprobación de esta capacitación.
Director / Gerente	06	Evalúan y deciden. En caso positivo, va al paso 07. En caso negativo, termina el proceso.
Jefe de Sistemas	07	Coordina ejecución de la capacitación.
Participante(s)	08	Recibe(n) la capacitación coordinada.

Participante	09	Una vez capacitado Firma la hoja de asistencia(Formato Libre)
Jefe de Sistemas	10	Archivará hoja de asistencia para constancia respectiva.
Jefe de Sistemas	11	Anualmente se evalúa la eficacia de la capacitación/entrenamiento tomada por sus colaboradores/usuarios y da retroalimentación para mejora.

Jefe de Sistemas controla el cumplimiento del Plan de Capacitación Anual.

REFERENCIAS:

Documento de Descripción de Funciones

DEFINICIONES:

REGISTROS:

Hoja de asistencia (Formato Libre)

Plan de Capacitación (Formato libre)

Registro del procedimiento: Asistencia técnica a usuarios.

Registro: Asistencia Técnica.

Tabla 7 Registro de asistencia técnica.

REGISTRO DE ASISTENCIA TÉCNICA
Fecha Solicita:_____ Fecha Entrega:_____
No:_____ Usuario_____ Área:_____
Datos del equipo:
Dispositivo: _____
Marca: _____ Modelo:_____
Serie: _____ Cod. Invent: _____
Descripción del problema (llenado por el Usuario)
_____
Revisión técnica
_____
_____
Solución al problema
_____
_____
_____
Firma Usuario

Registro del procedimiento: Mantenimiento de hardware / software de la información.

Registro: Control de mantenimiento de hardware y software

Se elaborado el cronograma de actividades a ejecutar y el cronograma de trabajo para el mantenimiento de los equipos de cómputo de las diferentes áreas y/o oficinas de la organización, el cual ha sido elaborado, teniendo en cuenta las actividades especificas de la oficina de Informática y que serán realizadas en el presente Plan de Trabajo.

Áreas		Semestre 1 (Fecha 1)	Semestre 2 (Fecha 2)
Gerencia	Planeado		
	Ejecutado		
Gestión de Calidad	Planeado		
	Ejecutado		
RRHH	Planeado		
	Ejecutado		
Operaciones	Planeado		
	Ejecutado		
Seguridad Electrónica	Planeado		
	Ejecutado		
Presupuesto	Planeado		
	Ejecutado		
Contabilidad	Planeado		
	Ejecutado		
Legal	Planeado		
	Ejecutado		
Ventas	Planeado		
	Ejecutado		
Sistemas	Planeado		
	Ejecutado		

Figura 2.7 Registro de control de mant. hardware y software.

Registro del procedimiento: Control de Backup de Base de Datos y Backup de la información.

Registro: Registro de control de Backup de la base de datos.

Sistemas Informáticos		ene-14	feb-14	mar-14	abr-14	may-14	jun-14	jul-14	ago-14	sep-14	oct-14	nov-14	dic-14
Sistemas financiero	Planeado												
	Ejecutado												
Sistema de roles	Planeado												
	Ejecutado												
Sistema de control de acceso	Planeado												
	Ejecutado												
Sistema de activos	Planeado												
	Ejecutado												

Figura 2.8 Registro de control de Backup de la base de datos.

Registro: Registro de control de Backup de la información de los equipos.

REGISTRO DE BACKUP DE INFORMACIÓN DEL USUARIO

Áreas		ene-14	feb-14	mar-14	abr-14	may-14	jun-14	jul-14	ago-14	sep-14	oct-14	nov-14	dic-14
Gerencia	Planeado												
	Ejecutado												
Gestión de Calidad	Planeado												
	Ejecutado												
RRHH	Planeado												
	Ejecutado												
Operaciones	Planeado												
	Ejecutado												
Seguridad Electrónica	Planeado												
	Ejecutado												
Presupuesto	Planeado												
	Ejecutado												
Contabilidad	Planeado												
	Ejecutado												
Legal	Planeado												
	Ejecutado												
Ventas	Planeado												
	Ejecutado												
Sistemas	Planeado												
	Ejecutado												

Figura 2.9 Registro de control de Backup de la información.

Registro del procedimiento: Capacitación al personal.

Registro: Plan de capacitación.

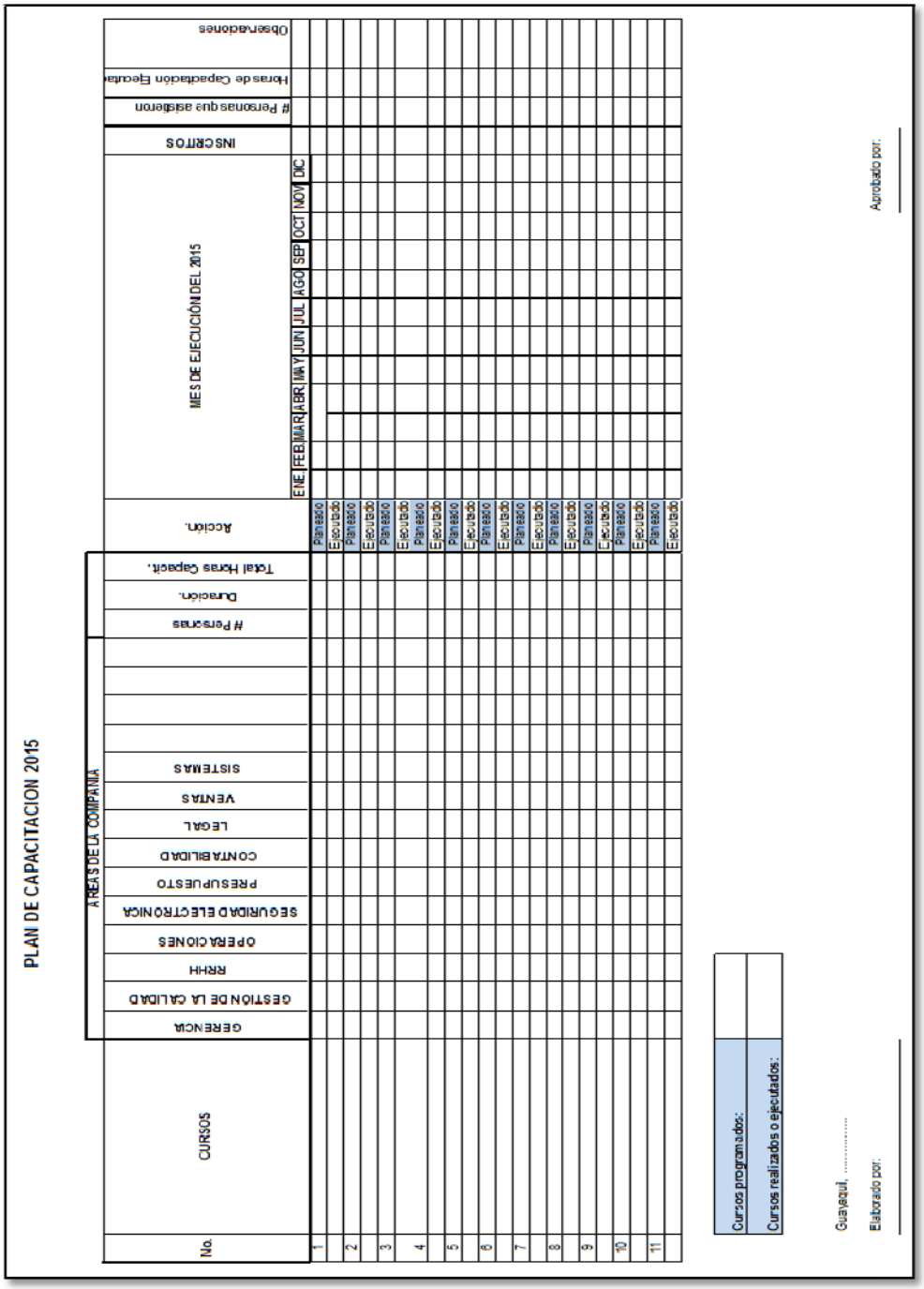


Figura 2.10 Creación de plan de capacitación.

CAPÍTULO 3

IMPLEMENTACIÓN Y PRUEBA DEL SISTEMA DE CALIDAD

3.1 Medición de los procesos claves

Para crear las mediciones, primero se debe evaluar el proceso, creando una ficha de proceso, dónde se define los procesos claves [5]. Véase en la figura 3.1.

La estructura de la ficha de proceso contiene:

Entrada: Son los requisitos del usuario, cliente o proveedor.

Salida: Servicios o productos.

Controles: Son los registros que necesita para que el proceso pueda cumplir con su meta.

Recursos: Son recursos humanos, infraestructura, ambiente de trabajo que se requiere para ejecutar el proceso.

Indicadores: Medición de los datos generados.

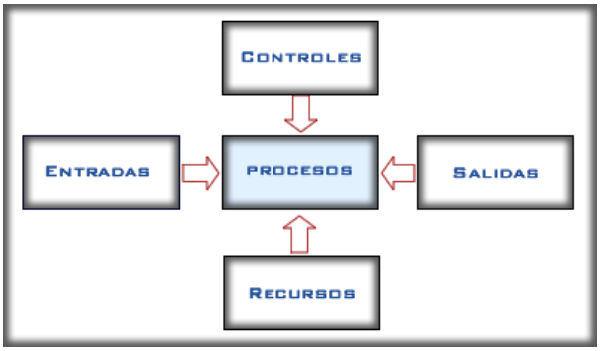


Figura 3.1 Estructura de la ficha de proceso.

Para evidenciar los resultados de los procesos se lo hace por medio de indicadores, se puede medir de 2 maneras: según el servicio que mide la eficiencia y el impacto sobre el usuario; y la otra manera es evaluar la eficacia en el desarrollo de un proceso [4].

En el capitulo anterior se estableció los procesos y se creó procedimiento para cumplir con los objetivos de la organización. Ahora se crea ficha de procesos claves.

A continuación, las fichas de procesos que nos ayuda a entender cómo realizar y obtener los resultados en los indicadores para luego interpretar el análisis.

Ficha de proceso: Servicios técnicos a usuarios.

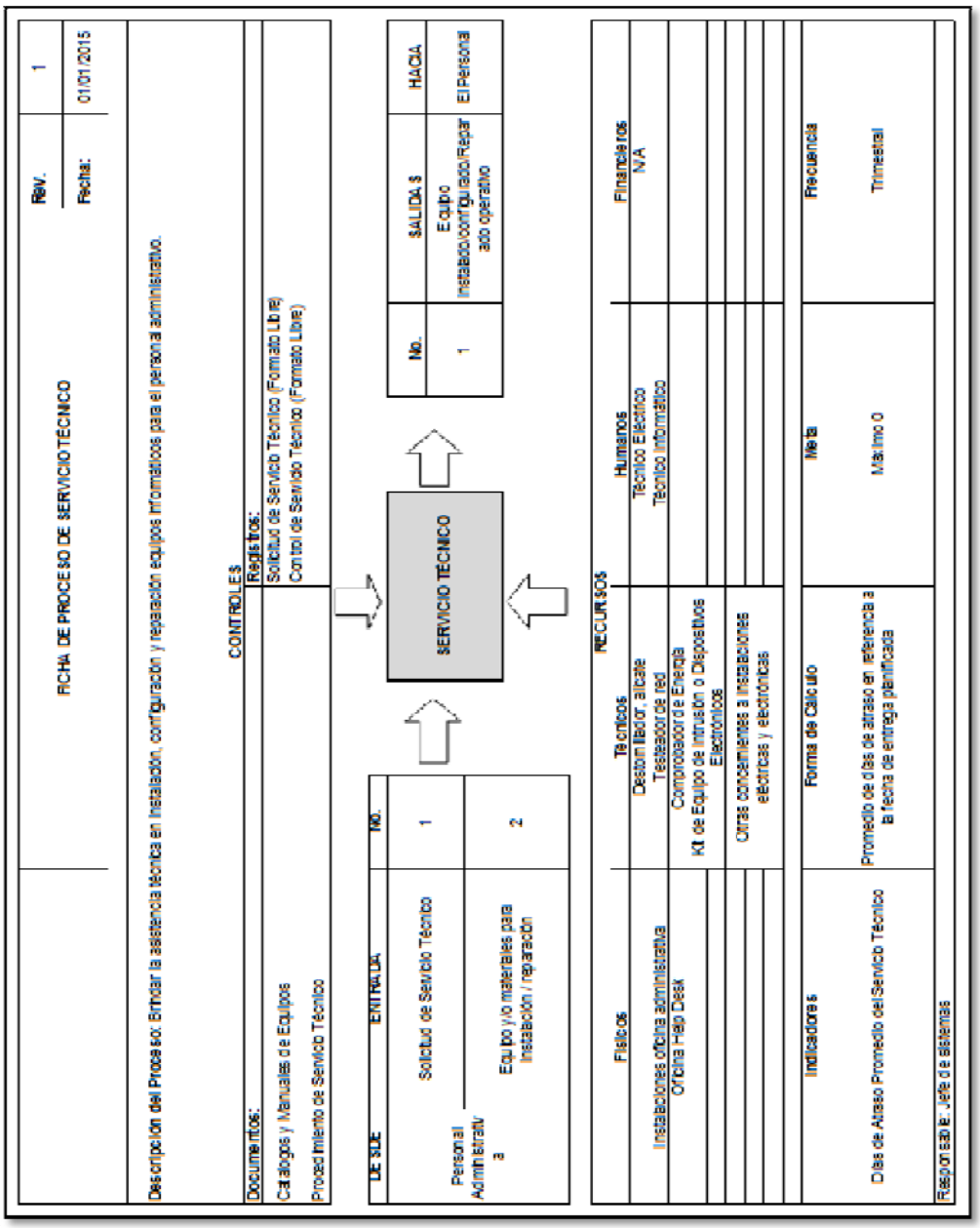


Figura 3.2 Ficha de servicios técnicos a usuarios.

Ficha de proceso: Control de Backup de Base de Datos y Backup de la información.

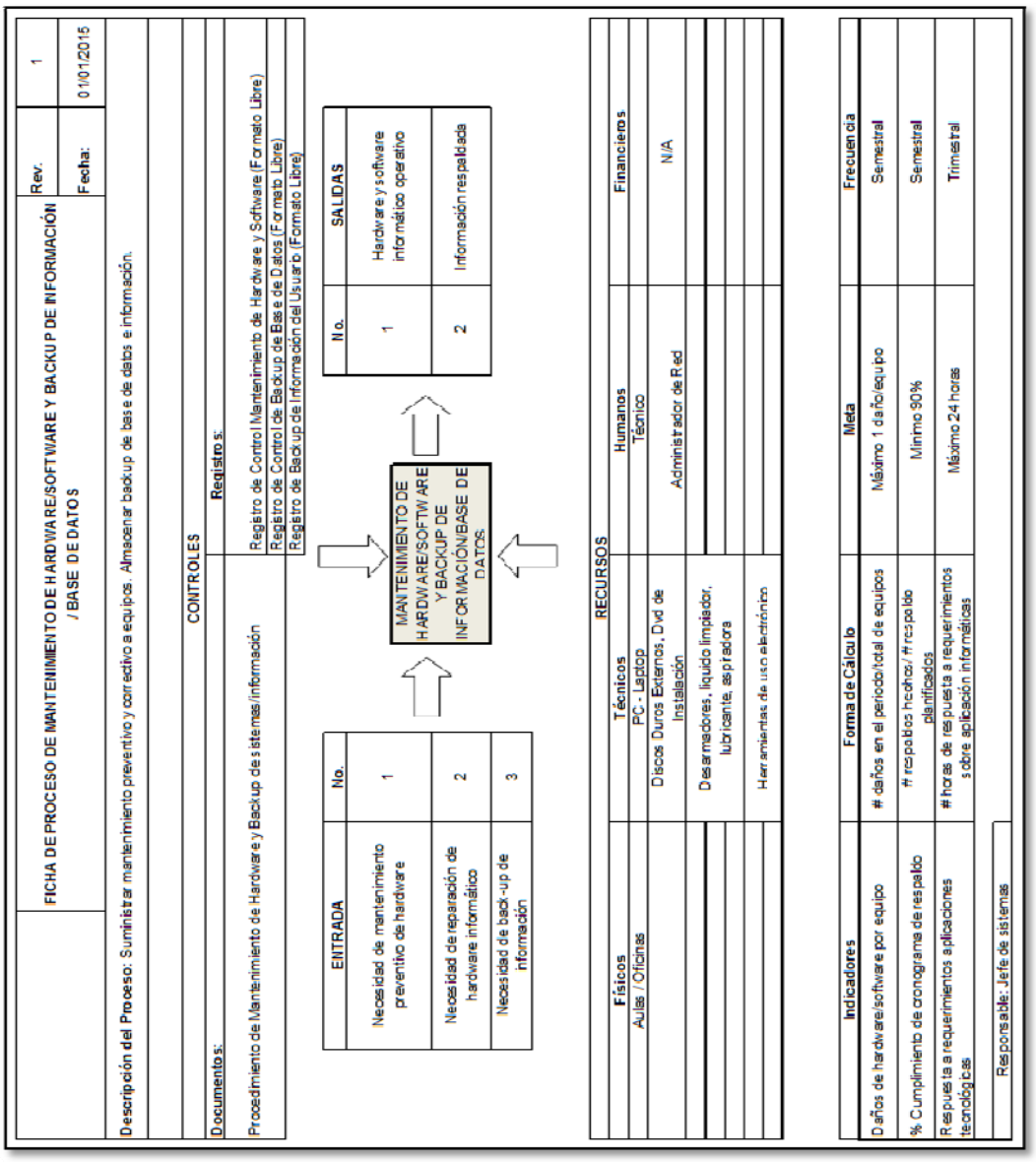


Figura 3.3 Ficha de proceso de control de backup DB/Información.

Ficha de proceso: Capacitación al personal.

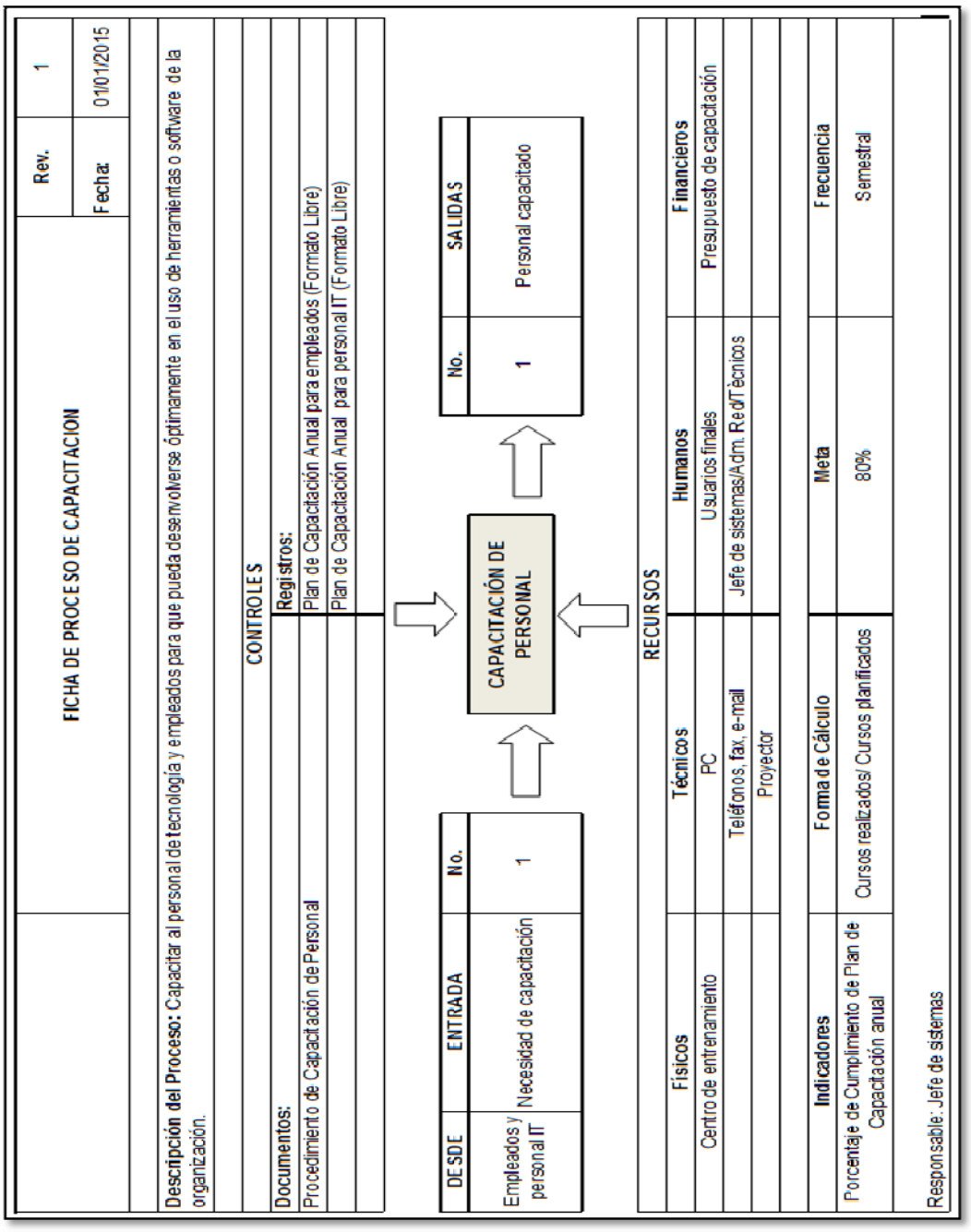


Figura 3.4 Ficha de proceso de Capacitación al personal.

Indicadores

Conforme al Sistema de Gestión de calidad el indicador nos muestra los resultados basándose en los datos obtenidos que nos permite compara con las metas propuestas puesto en la ficha de proceso, estos datos serán evaluados, analizados por el proceso y en caso de tener observaciones debe tomar acciones para cumplir con las metas.

Describir los campos del formato del indicador:

Proceso: Nombre de procesos claves.

Responsable: Empleado que cumplir con este proceso.

Indicador #: Puede existir más de un indicador de un proceso.

Forma de cálculo: Cálculo que mide el rendimiento del proceso.

Meta: Objetivo a cumplir con eficiencia.

Frecuencia: Tiempo de entrega de los indicadores.

Datos: Información a ser evaluada.

Análisis: Criterio después de ver los resultados, si se cumple o no la meta.

Acción a tomar: Correctivas para corregir o mejorar el proceso.

A continuación mostraremos los resultados de los indicadores, con su respectivo análisis y acciones a tomar.

3.2 Evidenciar el rendimiento del servicio técnico.

	REPORTE DE DESEMPEÑO DE PROCESOS	Código:	Formato Libre
		Fecha:	01-01-15
		Rev.	01

PROCESO: SERVICIO TÉCNICO AÑO: 2015
RESPONSABLE: JEFE TÉCNICO

INDICADOR 1: Días de atraso promedio del servicio técnico
FORMA DE CÁLCULO: Promedio de días de atraso en referencia a la fecha de entrega planificada
META: Máximo 0
FRECUENCIA: Trimestral
DATOS:

MES	Días de atraso Promedio del Sevicio Técnico
Enero - Marzo	0,43
Abril - Junio	0,57
Julio - Septiembre	0,00
Octubre - Diciembre	0,00

ANÁLISIS:
Hay un incremento en días falla.

ACCIONES A TOMAR:
Hay que mantener la política de análisis y prevención para mantenimiento los equipos en funcionamiento y evitar contratiempos en los servicios técnicos.

Figura 3.5 Indicador de servicio técnico.

3.3 Evidenciar el mantenimiento de equipos informáticos y backup.

	REPORTE DE DESEMPEÑO DE PROCESOS	Código:	Formato Libre
		Fecha:	01-01-15
		Rev.	01

PROCESO: MANTENIMIENTO DE HARDWARE , SOFTWARE Y BACKUP
RESPONSABLE: JEFE DE SISTEMAS

INDICADOR 1: Daños de hardware/software por equipo
FORMA DE CÁLCULO: # daños en el período/total de equipos
META: Máximo 1 daño/equipo
FRECUENCIA: Semestral
DATOS: 1er SEMESTRE 2015

AREA	# DAÑADO
Gerencia	0
Gestión de Calidad	0
RRHH	0
Operaciones	1
Seguridad Electrónica	0
Presupuesto	0
Contabilidad	1
Legal	1
Ventas	0
Sistemas	0
Total de daños	3
Total de equipos	42

# DAÑOS / EQUIPO = Total de daños en el período / Total de equipos	0,071428571

ANÁLISIS:
Se ha evidenciado 3 equipos dañados dentro de un período, debe cumplir con puntualidad el mantenimiento de equipos.

ACCIONES A TOMAR:
Mantener el mantenimiento de equipos.

Figura 3.6 Indicador de daños de hardware y software por equipo.

	REPORTE DE DESEMPEÑO DE PROCESOS	Código:	Formato Libre
		Fecha:	01-01-15
		Rev.	01

PROCESO: MANTENIMIENTO DE HARDWARE , SOFTWARE Y BACKUP
RESPONSABLE: JEFE DE SISTEMAS

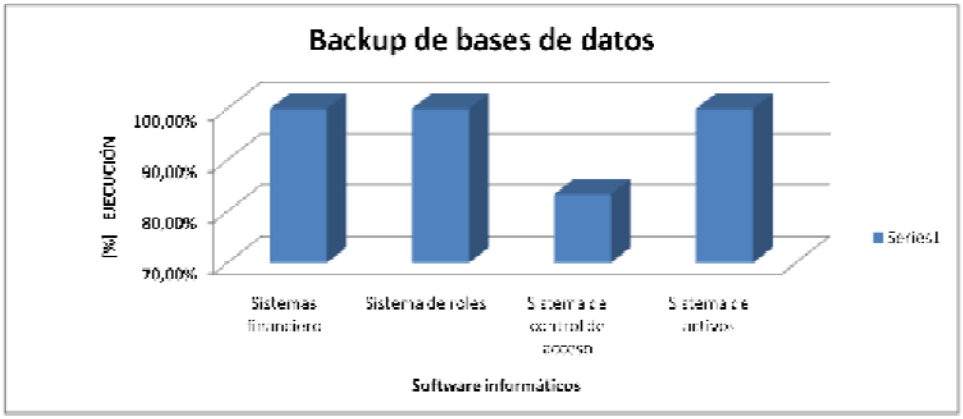
INDICADOR 2: % Cumplimiento de cronograma de respaldo
FORMA DE CÁLCULO: # respaldos hechos / # respaldo planificados
META: 90%
FRECUENCIA: SEMESTRAL

Control de Backup de Base de datos de Software informático

DATOS:

Backup Sistemas informático - 1do Semestre del 2015

Base de datos	Ejecutado
Sistemas financiero	100,00%
Sistema de roles	100,00%
Sistema de control de acceso	83,33%
Sistema de activos	100,00%



ANÁLISIS:
Problema con equipo de almacenamiento donde se almacenaba los registro de la base de datos de accesos, se fallo con lo planificado.

ACCIONES A TOMAR:
Se direccionó el backup a otro medio de almacenamiento, se agregar una observación al control donde debe existir redudancia en equipos sustanciales.

Figura 3.7 Indicador de backup de base de datos de sistemas inform.

	REPORTE DE DESEMPEÑO DE PROCESOS	Código: Formato Libre Fecha: 01-01-15 Rev. 01

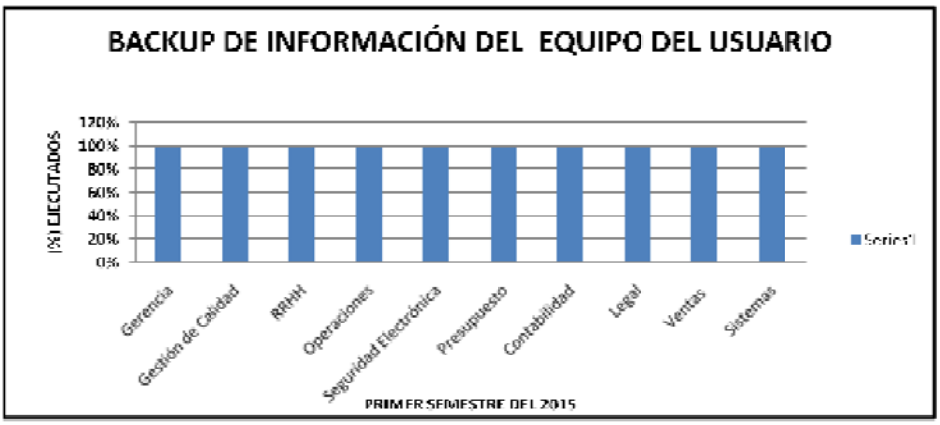
PROCESO: MANTENIMIENTO DE HARDWARE, SOFTWARE Y BACKUP
RESPONSABLE: JEFE DE SISTEMAS

INDICADOR 1: % Cumplimiento de cronograma de respaldo
FORMA DE CÁLCULO: # respaldos hechos / # respaldo planificados
META: 90%
FRECUENCIA: SEMESTRAL

Control de Backup de Base de información del equipo del usuario.

DATOS:
Backup de informático de información del usuario - 1do Semestre del 2015

	EJECUTADO
Gerencia	100%
Gestión de Calidad	100%
RRHH	100%
Operaciones	100%
Seguridad Electrónica	100%
Presupuesto	100%
Contabilidad	100%
Legal	100%
Ventas	100%
Sistemas	100%



ANÁLISIS:
Se cumple con la meta.
ACCIONES A TOMAR:
Seguir aplicando controles.

Figura 3.8 Indicador de backup de información de equipo de usuarios.

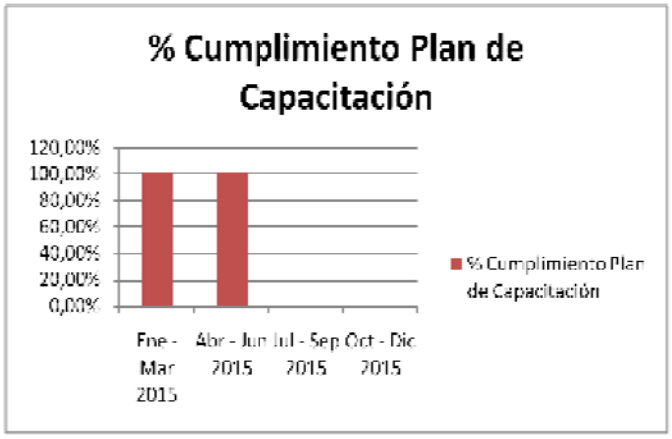
3.4 Evidenciar de la capacitación del personal de IT y administración.

	REPORTE DE DESEMPEÑO DE PROCESOS	Código:	Formato Libre
		Fecha:	01-01-15
		Rev.	01

PROCESO: CAPACITACIÓN DEL PERSONAL **AÑO: 2015**
RESPONSABLE: JEFE DE SISTEMAS

INDICADOR 1: Porcentaje de Cumplimiento de Plan de Capacitación anual
FORMA DE CÁLCULO: (Cursos realizados/cursos planificados) *100
META: 80%
FRECUENCIA: Trimestral
DATOS:

TRIMESTRE	% Cumplimiento Plan de Capacitación
Ene - Mar 2015	100,00%
Abr - Jun 2015	100,00%
Jul - Sep 2015	0,00%
Oct - Dic 2015	0,00%



ANÁLISIS:
Comparando los dos trimestres nos podemos dar cuenta que se han cumplido con lo planificado y programado al 100%.

ACCIONES A TOMAR:
Seguiremos cumpliendo con lo planificado en el plan de capacitacion anual para que el cumplimiento del plan de capacitacion trimestral calcule 100%.

Figura 3.9 Indicador del proceso capacitación del personal.

CONCLUSIONES Y RECOMENDACIONES

1. Conclusión: La implementación con SGSI nos permite identificar los procesos necesarios, aplicar controles para cumplir con los objetivos de la organización, además de mejorar dentro del mercado competitivo. Cabe recalcar que estas métricas de ayuda no se cumplirían si no está involucrada la dirección.

2. Conclusión: En esta tesis se ha procurado mejorar el servicio técnico a los usuarios, además de capacitarlos en el uso de herramientas tecnológicas, debido que el mayor fallo de la integridad de los datos proviene de su mal manejo.

3. Conclusión: Permite acoplar nuevos procesos, con el fin de mejorar el servicio, pero no olvide seguir con el estándar con que hasta el momento se ha usado.

4. Recomendación: Cualquier cambio en los procesos, procedimientos, funciones debe ser documentado y aprobados por la dirección.

5. Recomendación: Auditar los procesos, se recomienda al menos cada 6 meses. Nos permite conocer si están siguiendo los alineamientos de la norma.

6. Recomendación: Poner a prueba los procesos integrando ética hacking para conocer un riesgo reciente y probar la estabilidad de los controles.

7. Recomendación: Documentar los incidentes, será de aporte para establecer medidas, aplicar controles como contramedida.

BIBLIOGRAFÍA

[1]Órgano del Gobierno del Ecuador, Registro oficial, https://www.registroficial.gob.ec/, fecha del boletín 25 de septiembre del 2013, página 8.

[2]Portal ISO 2700 en español (ISO2700.es), ISO27K Toolkit, http://www.iso27000.es/herramientas.html - http://www.iso27001security.com/html/iso27k_toolkit.html, fecha publicada julio 2015.

[3]Estándar internacional ISO/IEC 27001:2005, Tecnología de la información – Técnicas de seguridad – sistemas de gestión de seguridad de la información – requerimientos, 15 de octubre 2005.

[4] UCA, Guía para la identificación y análisis de procesos, http://servicio.uca.es/personal/guia_procesos, septiembre 2007.

[5] Mtro. Gonzalo Guerrero Sánchez, Administración de procesos, http://es.slideshare.net/Gonzalo12345/gestin-por-procesos-9848472, Octubre 2011.