UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERIA

DIAGNÓSTICO DEL PLAN DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN UNA ORGANIZACIÓN

TESIS
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

PRESENTA

ANGELA MAZA CERÓN
COLVER CABRERA VILLANUEVA

DIRECTOR
ING. SERGIO NOBLE CAMARGO

CIUDAD UNIVERSITARIA 18/ 10/2013

DIAGNÓSTICO DEL PLAN DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN UNA ORGANIZACIÓN

Tabla de contenido

TABLA DE CONTENIDO

Introducción

INTRODUCCIÓN

El objetivo de este trabajo es obtener un Diagnóstico General del Plan de Seguridad en lo que se refiere a las Tecnologías de Información y Comunicaciones dentro de una Organización.

Las Organizaciones necesitan tener un buen nivel de seguridad en sus Tecnologías de Información y Comunicaciones, de esta forma lograrán protegerse ante riesgos que atenten contra la estabilidad de la operación. Es necesario contar con un plan de seguridad que cubra lineamientos que dicten los estándares tales como ISO 27002, COBIT e ITIL, entre otros, para establecer un óptimo Modelo de Seguridad.

Con este trabajo se busca analizar los Sistemas de Información para poder identificar y corregir vulnerabilidades, de manera que se minimicen después de la revisión de la infraestructura tecnológica con la que cuenta la Organización en cuestión.

La metodología aplicada consistió en desarrollar las siguientes actividades:

1. Investigación
    a. De normas.
    b. De estándares.
    c. De documentos.
    d. De manuales.
2. Comparación de las metodologías.
3. Identificar áreas de análisis.
    a. Administración
    b. Energía
    c. Control de Accesos
    d. Software
    e. Hardware
    f. Telecomunicaciones
4. Desarrollar un cuestionario diagnóstico.
    a. Creación y redacción del banco de preguntas.
    b. Selección de preguntas.
    c. Observación de las instalaciones, sistemas, cumplimiento de normas y procedimientos.
    d. Revisión analítica de:
        i. Documentación Técnica.
        ii. Manuales Técnicos (Instalación, Configuración)
        iii. Manuales de Usuario Final
        iv. Documentación Administrativa.
        v. Políticas y normas de actividad de sala.
        vi. Normas y procedimientos sobre seguridad física de los datos.
        vii. Contratos de seguros y de mantenimiento.
    e. Procesos de Operación
5. Identificar Organizaciones para aplicar el cuestionario.
    a. Dos universidades.
    b. Dos secretarías de gobierno.

    c. Una de diseño de software.
    d. Una de publicidad.
    e. Una tienda departamental.
6. Aplicación del cuestionario.
    a. Aplicación de la versión 1 a dos de las organizaciones.
7. Nuevas versiones del cuestionario.
    a. Aplicación de la versión 2 a todas las organizaciones.
    b. Aplicación de la versión final a todas las organizaciones.
8. Análisis de resultados.
9. Diagnóstico general.

El resultado que buscamos obtener es confirmar el nivel en que la Organización implementa su Plan de Seguridad. Así mismo con base en el diagnóstico obtenido proponer medidas correctivas para que la administración y operación sean óptimas.

Capítulo 1

CAPÍTULO I. FUNDAMENTOS TEÓRICOS

1.1 DEFINICIONES

Para el adecuado entendimiento de este trabajo a continuación se darán las definiciones de los términos más utilizados.

1. **Control de accesos**
   Conjunto de mecanismos y protocolos que se encargan de proteger física y lógicamente el acceso al Site verificando que la persona que ingresa sea quien dice ser.

2. **Diagnóstico**
   Análisis que se lleva a cabo con el objetivo de determinar cuál es la situación en que se encuentra la organización respecto a su seguridad informática.

3. **Energía**
   Se refiere al suministro adecuado de energía eléctrica necesario para que un sistema informático funcione.

4. **Hardware**
   Se refiere al equipamiento necesario para que un sistema informático funcione.

5. **Ingeniería**
   Conjunto de conocimientos y técnicas aplicadas a la creación, perfeccionamiento e implementación de sistemas lógicos y físicos que resuelven problemas cotidianos.

6. **Metodología**
   Conjunto de métodos que nos indican qué hacer y cómo hacerlo a fin de tener un control sobre lo que se va desarrollando.

7. **Organigrama**
   Representación gráfica de la estructura jerárquica de cualquier organización.

8. **Rol**
   Papel que desempeña una persona o un grupo de personas en cualquier actividad.

9. **Seguridad informática**
   Cualquier medida que ayude a prevenir la ejecución de operaciones no autorizadas sobre un sistema de información.

10. **Software**
    Componentes no físicos de un sistema informático, pueden ser sistemas operativos, programas y bases de datos.

11. Site

Nombre que se le da al centro de procesamiento de datos que es aquel lugar destinado a contener los recursos necesarios para procesar la información de una organización.

12. Telecomunicaciones

Sistemas que permiten la comunicación a larga distancia mediante el envío y recepción de datos.

1.2 METODOLOGÍAS MÁS POPULARES

1.2.1 COBIT(OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS)

En español COBIT se refiere a Objetivos de Control para Información y Tecnologías relacionadas, es un conjunto de prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA, en inglés Information Systems Audit and Control Association) y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés IT Governance Institute).[1]

Desarrolla, publica y promociona un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que estén autorizados y actualizados para el uso del día a día de los gestores de negocios y auditores.

Los auditores y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información y a decidir el nivel de seguridad y control que es necesario para proteger a las compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

Las organizaciones deben entender las ventajas de las tecnologías de información en el uso diario de sus operaciones y usar este conocimiento para aumentar el valor del negocio, para identificar la dependencia crítica de muchos procesos de negocio sobre las TI, como por ejemplo la necesidad de cumplir con estándares y normas. Para ayudar a las organizaciones satisfactoriamente en estas cuestiones, el ITGI ha publicado la versión 4.0 de la herramienta.

A. UTILIZACIÓN DE COBIT

COBIT para manejar los riesgos relacionados con el negocio:

- Selecciona, procesa y controla las TI apropiadas para la organización.
- Revisa la funcionalidad del plan de negocio de la organización.

[1] http://www.isaca.org/COBIT/Pages/default.aspx

- Evalúa los procedimientos y los resultados con las directrices de acuerdo con lo que establece COBIT.

- Evalúa el estado de la organización, identifica los factores de éxito críticos que miden el funcionamiento de las etapas y niveles de control.

De primera instancia, COBIT para su aplicación requiere de lo siguiente:

- Vincular las metas del negocio con las metas de las Tecnologías de Información (TI). Así mismo, organiza las actividades de las TI en un modelo de procesos.

- Identificar los principales recursos de las TI que guiarán los procesos (CMMI, CMM, ITIL).

COBIT cubre cuatro dominios (Ilustración 1):

1. Planificación y Organización. Se refiere al uso óptimo de la tecnología para que la organización alcance sus objetivos, se deben tomar en cuenta los siguientes objetivos:

    - Definir un plan de TI estratégico
    - Definir la estructura de la información
    - Determinar la infraestructura tecnológica
    - Definir los procesos de TI
    - Administrar la inversión en las TI
    - Comunicar los objetivos del plan estratégico
    - Administrar los recursos humanos de las TI
    - Administrar la calidad
    - Evaluar y maneja los riesgos de las TI
    - Administrar los proyectos

2. Adquisición e Implementación. Hace referencia a contar con un plan de mantenimiento para prolongar la vida del sistema de información con el que cuenta la organización, para ello hay que llevar a acabo lo siguiente:

    - Identificar las soluciones que pueden ser automatizadas
    - Adquirir y dar mantenimiento al software
    - Adquirir y dar mantenimiento a la infraestructura tecnológica
    - Facilitar la operación e implementación de la tecnología
    - Administrar los recursos de las TI
    - Administrar los cambios
    - Instalar y aprobar las soluciones y los cambios

3. Entrega y soporte. Se enfoca en los procesos de apoyo que ayudan a uso eficiente de los sistemas de TI, tomando en cuenta lo siguiente:

    - Definir y administrar los niveles de servicio
    - Administrar los servicios de terceros

- Administrar el funcionamiento y la capacidad
- Asegurar el servicio continuo
- Asegurar la seguridad de los sistemas
- Identificar y asignar los gastos
- Entrenar a los usuarios
- Administrar una bitácora de servicios e incidentes que se presenten
- Administrar la configuración del sistema de TI
- Administrar los problemas
- Administrar los datos
- Administrar el ambiente físico
- Administrar las operaciones

4. Supervisión y evaluación. Cubre el aspecto de evaluar la eficiencia del sistema TI, para lo cual es necesario lo siguiente:

    - Supervisar y evaluar los procesos de TI
    - Supervisar y evaluar el control interno
    - Asegurar el cumplimiento
    - Administrar adecuadamente las TI

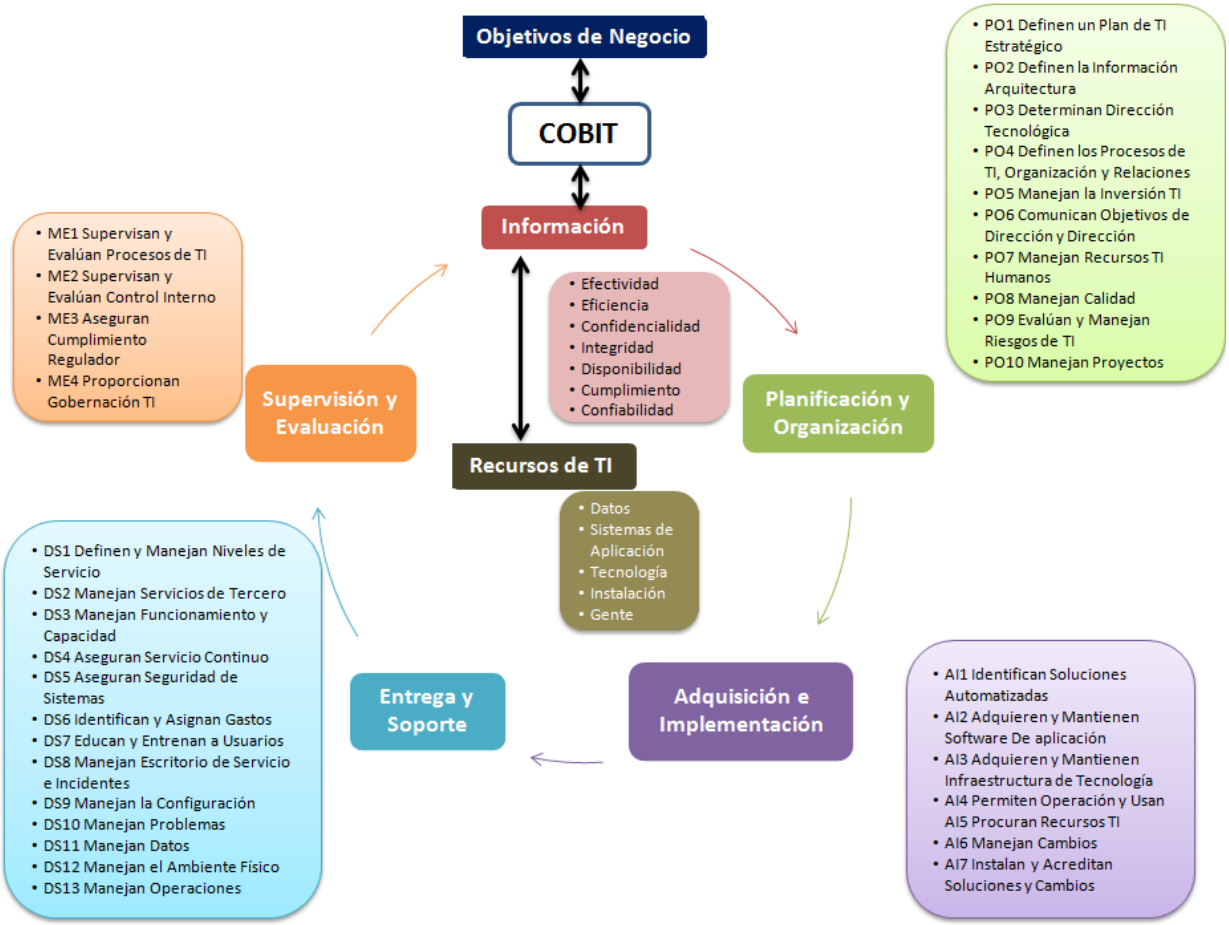


Ilustración 1. Dominios y procesos de COBIT

RESULTADO ESPERADO

La metodología COBIT se utiliza para implementar, controlar y evaluar las Tecnologías de Información y Comunicación; añadiendo objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez. [2]

Permite a las Organizaciones aumentar su productividad en las Tecnologías de Información y Comunicación (TIC's) y reducir los riesgos tecnológicos a partir de parámetros aplicables y aceptados y para mejorar las prácticas de planeación, control y seguridad de las TIC's.

COBIT contribuye a reducir las diferencias entre los objetivos de negocio, los beneficios, los riesgos, el control y los aspectos técnicos de las TIC's proporcionando un marco Referencial para su dirección efectiva.

B. RESUMEN EJECUTIVO

El resumen ejecutivo de COBIT consiste en una descripción ejecutiva que proporciona una ayuda al entendimiento de los conceptos clave de COBIT y sus principios.

Así mismo, incluye un resumen del marco que proporciona un entendimiento más detallado de estos conceptos clave y sus principios, identificando los cuatro dominios del COBIT (Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y, Supervisión y Evaluación) y los 34 procesos de TI.

C. MARCO

Una organización es construida sobre un marco sólido de datos e información. El marco explica cómo se entrega la información en cada proceso de TI y cómo el negocio tiene que alcanzar sus objetivos. Esta entrega es controlada por 34 objetivos de control de alto nivel, uno para cada proceso de TI contenido en los cuatro dominios.

El marco identifica los criterios de seguridad de la información (la eficacia, la confidencialidad, la integridad, la disponibilidad, el cumplimiento y la fiabilidad), así como qué recursos de las TI (la gente, los usos, la tecnología, las instalaciones y los datos) son importantes para los procesos de TI con el fin de apoyar totalmente el objetivo de negocio.

D. OBJETIVOS DE CONTROL

Los objetivos de control de COBIT brindan métricas y modelos de madurez para medir los logros, e identifican las responsabilidades asociadas de los propietarios de los procesos de negocio y de las TI.

Se incluyen las declaraciones de resultados deseados u objetivos para ser alcanzados y poniendo en práctica los objetivos de control específicos, detallados en los 34 procesos de las TI.

[2] http://www.itera.com.mx/itinstitute/mails/chile/cobit.htm

E. DIRECTRICES DE AUDITORÍA

Las directrices de auditoria ayudan a asignar responsabilidades y medir el desempeño, aconsejando una serie de actividades a realizar de acuerdo con los 34 objetivos de control de las TI. Ayudan a identificar y asesorar en qué casos los controles son suficientes y cuándo los procesos requieren ser mejorados.

F. INSTRUMENTO DE PUESTA EN PRÁCTICA

Un instrumento de puesta en práctica debe contener los siguientes puntos:

- El diagnóstico de control de las TI.
- Preguntas frecuentes.
- Casos de estudio de organizaciones
- Las presentaciones de diapositivas que pueden ser usadas para introducir COBIT en organizaciones.

Está diseñado para facilitar la puesta en práctica de COBIT en los ambientes de trabajo

G. DIRECTRICES DE DIRECCIÓN

Las directrices de dirección han sido desarrolladas para determinar si los objetivos de control están debidamente implementados. Sus objetivos son: la administración del desempeño, la seguridad y el control de la información.

Las directrices de dirección están compuestas por:

- **Modelos de Madurez,** ayudan a determinar las etapas y los niveles de expectativas de control y compararlos contra normas usadas en la industria.

- **Factores Críticos de Éxito** (CSFs, siglas de los términos en inglés), identifican las acciones más importantes para alcanzar el control de los procesos de las TI.

- **Indicadores Clave de Objetivos** (KGIs, siglas de los términos en inglés), definen los niveles óptimos de funcionamiento.

- **Indicadores Claves de Desempeño** (KPIs, siglas de los términos en inglés) miden cómo un proceso de control de las TI cumple su objetivo.

Las directrices de dirección están orientadas a resolver preocupaciones de área de administración[3] como las siguientes:

- Medición del desempeño - ¿Cuáles son los indicadores de un buen desempeño?

- Determinación del perfil de control de las TI - ¿Qué es importante? ¿Cuáles son los Factores Críticos de Éxito para el control?

- Conocimiento o concientización - ¿Cuáles son los riesgos de no alcanzar nuestros objetivos?

[3] IT Governance Institute. "Cobit. Directrices Gerenciales".3ª.ed. Julio: 200. Pág. 5-7.

- Benchmarking - ¿Qué hacen los demás? ¿Cómo medimos y comparamos?

1.2.2 COSO(COMITÉ DE ORGANIZACIONES PATROCINADORAS DE LA COMISIÓN TREADWAY)

La implementación de COSO (en español Comité de Organizaciones Patrocinadoras de la Comisión Treadway) en las organizaciones permite llevar a cabo una evaluación continua del control interno en la preparación de estados financieros, para que de esta manera se asegure la efectividad y eficiencia en las operaciones, seguridad de la información financiera, cumplimiento de leyes y regulaciones, así como salvaguardar los activos (Ilustración 2).

El control interno es tomado como un proceso, el cual consta de una serie de acciones, modificaciones o funciones que en conjunto logran un resultado. Todo esto recae en el personal y se debe estar al pendiente de los riesgos y controles para poder resolverlos adecuadamente.

Este método indica lo importante que es entender que existen limitaciones en el control interno ya que no se puede tener un control para prevenir cada problema que se presente siendo que el aspecto más importante es el cumplimiento de los objetivos.

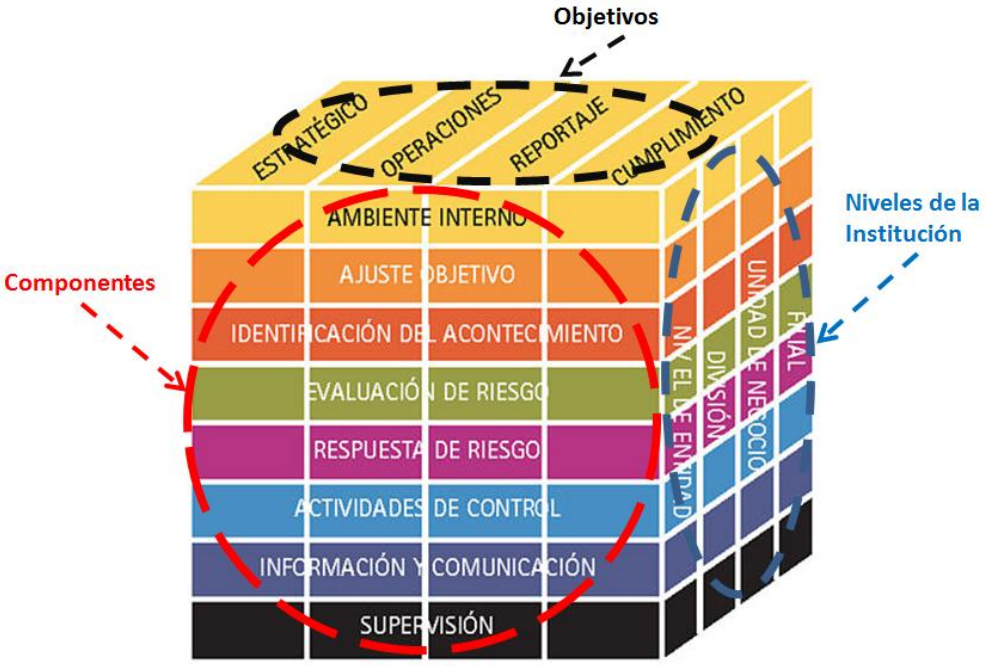


Ilustración 2. ¿Qué es COSO?[4]

En el control interno se identifican tres categorías de objetivos: **operaciones eficientes, reporte financiero y cumplimiento de regulaciones**, y cinco componentes, los cuales son:

[4] http://imgs.wke.es/0/9/5/1/im0000280951.jpg/

1. **Ambiente de control**. Es considerado el más importante debido a que radica en la integridad y competencia del personal de la organización, es importante contar con personal competente, ya que debe ser responsable de sus acciones.

2. **Evaluación de riesgos**. Se enfoca a identificar y analizar los riegos internos o externos, prestando atención a los siguientes puntos[5]:

    - Avances tecnológicos, sistemas o procedimientos en situación de cambio.
    - Nuevas líneas de negocio, productos, actividades o funciones.
    - Reestructuración corporativa.
    - Expansión o adquisición de operaciones extranjeras.
    - Personal de nuevo ingreso o rotación de los existentes.
    - Índices de Crecimiento.

3. **Actividades de control**. Se llevarán a cabo una vez conociendo los riesgos a contrarrestar y se agrupan de acuerdo con dos criterios:

    Objetivos
    - Operaciones
    - Confiabilidad de la información financiera
    - Cumplimiento de leyes y reglamentos

    Tipo de control
    - Preventivo/Correctivo
    - Manuales/Automatizados o Informáticos.
    - Gerenciales o Directivos.

4. **Información y comunicación**. Se encamina a contar con la información periódica y oportuna para orientar las acciones que se llevarán a cabo para alcanzar los objetivos de la organización.

5. **Monitorizar**. Su función es cerciorarse de que el control interno se realiza debidamente a través de actividades continuas de supervisión o evaluación.

Estos componentes se ampliaron a 8 en la actualización del informe COSO del 2004[6], quedando los componentes siguientes:

1. Ambiente de Control.
2. Establecimiento de Objetivos.(**nuevo**)
3. Identificación de Eventos.(**nuevo**)

[5] MORENO, Perdomo Abraham. "Fundamentos de Control Interno". 9ª.ed. THOMSON. Colombia: 2004, pág. 236.
[6] http://www.coso.org/default.htm

4. Evaluación de Riesgos.
5. Respuesta al Riesgo.(**nuevo**)
6. Actividades de Control.
7. Información y Comunicación.
8. Monitorizar.

RESULTADO ESPERADO

Se utilizan varias metodologías y herramientas de evaluación, incluyendo listas de comprobación, cuestionarios, cuadros estadísticos y técnicas de diagramas de flujo. Con base en esto se genera un informe aunado a la recopilación de datos ya sean presupuestos, estados financieros, reglamentos, etc. Se presentan los resultados de los datos obtenidos mediante entrevistas, encuestas y observación durante la investigación y con base en esto se obtiene un indicador para ver el resultado y facilitar el análisis.

APARTADOS QUE REVISA

1) **Ambiente de Control**
    a. Filosofía de la administración de riesgos.
    b. Integridad y valores éticos.
    c. Compromiso profesional.
    d. Estructura organizacional.
    e. Asignación de autoridad y responsabilidad.
    f. Políticas y prácticas de recursos humanos.

2) **Establecimiento de Objetivos.**
    a. Objetivos estratégicos. Describen el alcance, estilo e ideales de una organización a mediano y largo plazo.
    b. Objetivos relacionados. Vinculados e integrados con otros objetivos específicos.
    c. Riesgo aceptado y Niveles de tolerancia. Costo que está dispuesto a asumir la organización para alcanzar su misión y visión.

3) **Identificación de Eventos.** Utiliza las siguientes técnicas:

   a. Identificación de eventos. Listados de eventos posibles en un área específica.
   b. Talleres de trabajo. El objetivo es aprovechar el conocimiento colectivo.
   c. Entrevistas. Para averiguar las opiniones y conocimientos del entrevistado.
   d. Cuestionarios y encuestas. Centradas en factores internos y externos que pueden dar lugar a un evento.
   e. Análisis del flujo de procesos. Se refiere a una representación esquemática de un proceso, con esto se busca comprender las relaciones y responsabilidades de cada componente.
   f. Principales indicadores de eventos e indicadores de alarma. Mediciones cualitativas y cuantitativas para un mejor conocimiento de posibles riesgos.
   g. Seguimiento de datos de eventos con pérdidas.
   h. Identificar los eventos.
   i. Identificar la relación de los nuevos eventos que pueden afectar a los objetivos

4) Evaluación de Riesgos.

   a. Técnicas probabilísticas.

   b. Metodologías no probabilísticas.

   c. Benchmarking.

5) Respuesta al Riesgo.

   a. Evitar el riesgo mediante actividades.

   b. Reducir acciones para reducir la posibilidad del riesgo.

   c. Compartir con terceras partes para reducir el riesgo, como contratar un seguro.

   d. Aceptar el riesgo y no llevar a cabo una acción que afecte el impacto del riesgo.

6) Actividades de Control.

   a. Análisis efectuados por la dirección.

   b. Gestión directa de funciones por actividades.

   c. Proceso de información. Controles para comprobar exactitud, totalidad y autorización de transacciones.

   d. Controles físicos. Relativo a los inventarios.

e. Indicadores de rendimiento.
f. Segregación de funciones. Reparto de actividades entre los empleados.

7) Información y Comunicación.

8) Monitorizar.

a. Actividades continuas.

b. Evaluaciones puntuales.

1.2.3 ITIL(BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN)

La Biblioteca de Infraestructura de Tecnologías de Información, abreviada ITIL es una metodología enfocada a la gestión de servicios de las TI, orientada al control, operación y administración de los servicios, garantizando la calidad y eficiencia en las operaciones y la satisfacción del cliente a un costo manejable. Recomienda que para toda actividad que se realice se deba generar la documentación adecuada.

Cabe aclarar que en esta metodología sólo se certifican personas, para ello se debe acudir a las instituciones ISEB (Information Systems Examination Board) y EXIN (Examination for Information Science in the Netherlands) en las cuales, se debe aprobar el examen que corresponde a cada nivel (Ilustracion 3).

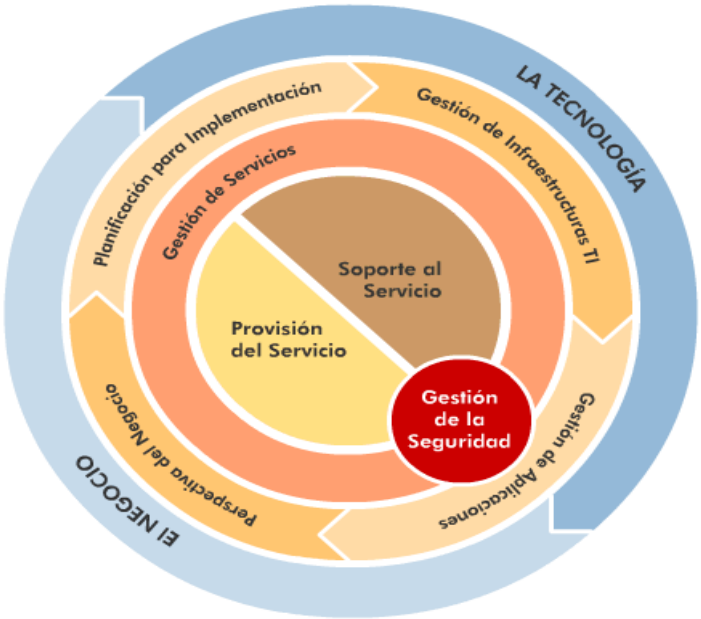


Ilustración 3. Estructura de ITIL

Sus principales secciones son:

- Estrategia del Servicio
- Diseño del Servicio
- Transición del Servicio
- Operación del Servicio
- Mejora Continua del Servicio

Las cuales describen 26 procesos básicos para la mejora continua de los servicios.

ITIL postula que el servicio de soporte, la administración y la operación se realizan a través de cinco procesos:

1. **Manejo de incidentes**. Su principal objetivo es restablecer el servicio de la forma más rápida y eficazmente posible de manera que el cliente no lo perciba y no sea afectado. Lo óptimo es que el cliente no perciba las fallas que se presenten en el sistema, a esto se le conoce como disponibilidad del servicio, este proceso cuenta con fases en donde se manejan cuatro pasos básicos: incidencia, monitorización, manejo de secuencias y comunicación.

2. **Manejo de problemas**. Su propósito es prevenir y reducir lo más que se pueda los incidentes que se presentan, además, debe proporcionar soluciones rápidas y certeras para asegurar el uso estructurado de los recursos. Se manejan dos fases: Una relacionada con el control del problema y la otra con el control del error.

3. **Manejo de configuraciones**. Su intención es proporcionar información real de lo que se encuentra configurado e instalado en el sistema del cliente. Está relacionado con cuatro fases: administración de cambios, administración de liberaciones, administración de configuraciones y administración de procesos diversos.

4. **Manejo de cambios**. Su meta es reducir en la medida de lo posible los riesgos técnicos, económicos y de tiempo a la hora de realizar los cambios, a lo largo de este proceso se da una fase de monitorización para ver que no hubo una desviación del objetivo.

5. **Manejo de entregas**. Su finalidad es la planeación y control de la instalación de software y hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente de producción.

RESULTADO ESPERADO

Se utilizan los Indicadores Clave de Rendimiento ITIL (KPI's, del inglés Key Performance Indicators) para evaluar si los procesos que han sido implantados en una organización funcionan de acuerdo con lo esperado. Estos son definidos conforme a lo que se considera una ejecución exitosa de un proceso, estas definiciones varían acordes con la naturaleza de la organización y a la importancia de cada proceso.

Sin embargo, se cuenta con una cantidad de KPI's típicos para evaluar los procesos de ITIL. Una buena definición de las métricas inicia cuando van de la mano los objetivos del negocio con los objetivos de la organización, en caso contrario no se podrán marcar los beneficios por parte de la implantación de los procesos de servicio de soporte y la prestación de servicios.

Un principio extensamente aceptado mantiene que los "KPI´s deben ser:

- Específico (**S**pecific)
- Medible (**M**easurable)
- Alcanzable (**A**chievable)
- Orientado a resultados (**R**esult-oriented)
- Terminados a tiempo (**T**imely)

Consiste en los siguientes Indicadores Clave de Rendimiento ITIL:

KPI's ITIL - Estrategia del Servicio

- KPI's Gestión del Portafolio de Servicios

KPI	Descripción
Cantidad de nuevos servicios planeados	▪ Porcentaje de nuevos servicios desarrollados a iniciativa de la gestión del portafolio de servicios
Cantidad de nuevos servicios no planeados	▪ Porcentaje de nuevos servicios desarrollados sin la iniciativa de la gestión del portafolio de servicios
Cantidad de iniciativas estratégicas	▪ Cantidad de iniciativas estratégicas lanzadas por el proceso de la gestión del portafolio de servicios
Cantidad de clientes nuevos	▪ Cantidad de clientes nuevos adquiridos
Cantidad de clientes perdidos	▪ Cantidad de clientes perdidos a competidores que proveen servicios

- KPI's Gestión Financiera

KPI	Descripción
Ajustarse al presupuesto	▪ Definir el porcentaje de proyectos a desarrollar de acuerdo al presupuesto de TI.
Estimación de costo/ beneficio	▪ Porcentaje de archivos de proyecto que contiene estimaciones de costo-/beneficio.
Revisión post implementación	▪ Porcentaje de proyectos donde los costos y beneficios se verifican después de la implementación.
Ajustarse al presupuesto aprobado	▪ Porcentaje de gastos de TI que excede el presupuesto aprobado.
Ajustarse a los recursos del proyecto	▪ Porcentaje de gastos que exceden el presupuesto de TI planificado para el proyecto.
Propuestas para optimización de costo	▪ Cantidad de propuestas de la gestión financiera para el uso óptimo de recursos financieros.

KPI's ITIL - Diseño del Servicio

- KPI's Gestión del Nivel de Servicio (SLM)

KPI	Descripción
Servicios cubiertos	▪ Cantidad de servicios cubiertos
Servicios monitorizados	▪ Cantidad de servicios monitorizados que reportan puntos débiles.
Servicios bajo revisión	▪ Cantidad de servicios revisados regularmente.
Cumplimiento de niveles de servicio	▪ Cantidad de servicios que cumplen con los niveles de servicio acordados.
Cantidad de asuntos de Servicio	▪ Cantidad de asuntos, al proveer servicios, que son identificados y tratados en un plan de mejoras al servicio.

- KPI's Gestión de la Disponibilidad

KPI	Descripción
Disponibilidad de servicio	▪ Servicios en relación a la disponibilidad.

Cantidad de interrupciones de servicio	▪ Cantidad de interrupciones de servicio.
Duración de interrupciones de servicio	▪ Duración promedio de interrupciones de servicio.
Monitorización de disponibilidad	▪ Porcentaje de servicios y componentes de infraestructura sujetos a monitorización.
Medidas de disponibilidad	▪ Cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad.

- KPI's Gestión de la Capacidad

KPI	Descripción
Incidentes debidos a falta de capacidad	▪ Cantidad de incidentes ocurridos debido a insuficiencia de capacidad de servicios o capacidad de componentes
Exactitud del pronóstico de la capacidad	▪ Desviación del objetivo curso real.
Ajustes a la capacidad	▪ Cantidad de ajustes a la capacidad de servicios y capacidad de componentes debido a cambios en la demanda
Ajustes a la capacidad no planeados	▪ Cantidad de aumentos no planeados a la capacidad de servicios o capacidad de componentes como resultado de limitaciones de capacidad
Tiempo para la resolución de carencias en la capacidad	▪ Tiempo empleado para la resolución de una limitación detectada en la capacidad
Reservas de capacidad	▪ Porcentaje de reservas de capacidad en tiempos de demanda normal y máxima
Porcentaje de monitorización de capacidad	▪ Porcentaje de servicios y componentes de infraestructura monitorizados para capacidad

- KPI's Gestión de la Continuidad del Servicio de las TI (ITSCM)

KPI	Descripción
Procesos de negocio con acuerdos de continuidad	▪ Porcentaje de procesos de negocio cubiertos por metas específicas de continuidad del servicio
Opciones en preparación para desastres	▪ Cantidad de opciones identificadas en la preparación para eventos de desastres
Duración de la	▪ Duración desde la identificación del riesgo

implementación	relacionado a desastres hasta la implementación de un mecanismo de continuidad adecuado
Cantidad de prácticas para desastres	▪ Cantidad de prácticas para desastres que realmente se llevaron a cabo
Cantidad de defectos identificados durante las prácticas para desastres	▪ Cantidad de defectos identificados en la preparación para eventos de desastres identificados durante las prácticas

- KPI's Gestión de la Seguridad de las TI

KPI	Descripción
Cantidad de medidas preventivas implementadas	▪ Cantidad de medidas de seguridad preventivas implementadas como respuesta a amenazas de seguridad identificadas.
Duración de la implementación de medidas preventivas implementadas	▪ Duración desde la identificación de una amenaza de seguridad hasta la implementación de una contramedida adecuada.
Cantidad de incidentes graves de la seguridad	▪ Cantidad de incidentes de seguridad identificados, clasificados por categoría de gravedad.
Cantidad de periodos de inactividad de servicio relacionados con la seguridad	▪ Cantidad de incidentes de seguridad que causan interrupciones de servicio o disponibilidad reducida.
Cantidad de pruebas de seguridad	▪ Cantidad de pruebas y adiestramientos de seguridad llevados a cabo.
Cantidad de defectos identificados durante las pruebas de seguridad	▪ Cantidad de defectos identificados en los mecanismos de seguridad durante las pruebas.

- KPI's Gestión de Proveedores

KPI	Descripción
Cantidad de proveedores acordados	▪ Porcentaje de contratos.
Cantidad de revisiones de contratos	▪ Cantidad de revisiones de contratos y proveedores.
Cantidad de incumplimientos de contrato identificados	▪ Cantidad de obligaciones contractuales que no cumplieron los proveedores.

KPI's ITIL - Transición del Servicio

- KPI's Gestión de Cambios

KPI	Descripción
Cantidad de cambios mayores	▪ Cantidad de cambios mayores evaluados por el consejo consultor para cambios.
Cantidad de reuniones de Consejo Consultor para Cambios	▪ Cantidad de reuniones con consultor para cambios.
Tiempo para autorización para cambios	▪ Tiempo medio transcurrido desde la solicitud de una solicitud de cambio a la gestión de cambios hasta la autorización para el cambio.
Tasa de aceptación de cambios	▪ Cantidad de cambios aceptados vs. rechazados.
Cantidad de cambios urgentes	▪ Cantidad de cambios urgentes evaluados por el consejo consultor para cambios de emergencia.

- KPI's Gestión de Proyectos (Planificación y Soporte Transición)

KPI (Métrica de CSI)	Descripción
Cantidad de proyectos	▪ Cantidad de despliegues de ediciones bajo el control de la gestión de proyectos
Porcentaje de proyectos con Declaración de Proyecto	▪ Porcentaje de proyectos que comienzan con declaración de proyecto ya firmada
Cantidad de cambios a la Declaración de Proyecto	▪ Cantidad de cambios a la Declaración de Proyecto luego de comenzado el proyecto
Adherencia a presupuesto del proyecto	▪ Uso de recursos humanos y financieros, reales vs. planificadas
Retrasos del proyecto	▪ Fechas de finalización de proyecto, real vs. planificadas.

- KPI's Gestión de Versiones e Implementación

KPI	Descripción
Cantidad de ediciones	▪ Cantidad de ediciones desplegadas en el área de producción de TI, agrupadas en ediciones mayores

	(importantes, sujetas a riesgos) o menores
Duración de Ediciones Mayores	▪ Duración media de ediciones mayores, desde su autorización hasta su finalización
Cantidad de retrocesos de ediciones	▪ Cantidad de ediciones que fueron revertidas
Proporción de ediciones de despliegue automático	▪ Proporción de nuevas ediciones distribuidas automáticamente.

- KPI's Validación y Pruebas de Servicios

KPI	Descripción
Porcentaje de fracasos de pruebas de aceptación de componentes de ediciones	▪ Porcentaje de componentes de ediciones que no pasa las pruebas de aceptación
Cantidad de errores identificados	▪ Cantidad de errores identificados durante las pruebas de ediciones por edición
Tiempo para corregir un error	▪ Tiempo necesario para corregir los errores identificados durante las pruebas de ediciones
Incidentes causados por ediciones nuevas	▪ Cantidad de incidentes atribuibles a ediciones nuevas
Porcentaje de fracasos de pruebas de aceptación de servicio	▪ Porcentaje de pruebas de aceptación de servicio que no son aprobadas por el cliente

- KPI's Activos de Servicio y Gestión de la Configuración

KPI	Descripción
Frecuencia de verificación	▪ Frecuencia de verificaciones físicas o de configuración
Duración de verificación	▪ Duración promedio de verificaciones físicas del contenido.
Esfuerzo para verificaciones	▪ Promedio de esfuerzo de trabajo para verificaciones físicas del contenido
Porcentajes de gestión	▪ Porcentaje de elementos de configuración de la gestión.
Actualización automática	▪ Porcentaje de elementos de configuración actualizan automáticamente

Cantidad de errores	▪ Número de ocasiones en las que se detectaron incorrecciones

KPI's ITIL - Operación del Servicio

- KPI's Gestión de Incidentes

KPI	Descripción
Cantidad de incidentes repetidos	▪ Cantidad de incidentes repetidos con métodos para su resolución ya conocidos
Incidentes resueltos a distancia	▪ Cantidad de incidentes resueltos a distancia por la bitácora de servicios.
Cantidad de escalados	▪ Cantidad de escalados de incidentes no resueltos en el tiempo acordado
Cantidad de incidentes	▪ Cantidad de incidentes registrados por la bitácora de servicios.
Tiempo de resolución de incidente	▪ Tiempo promedio para resolver incidentes agrupados por categorías.
Tasa de Resolución de Primera Llamada	▪ Porcentaje de incidentes resueltos en el bitácora de servicios durante la primera llamada,
Resolución a tiempo	▪ Porcentaje de incidentes resueltos durante el tiempo acordado.
Esfuerzo de resolución de incidente	▪ Promedio de esfuerzo de trabajo para resolver Incidentes.

- KPI's Gestión de Problemas

KPI	Descripción
Cantidad de problemas	▪ Cantidad de problemas registrados por la gestión de problemas.
Tiempo de resolución de problemas	▪ Tiempo promedio para resolver problemas.
Cantidad de incidentes por problema	▪ Cantidad promedio de incidentes vinculados al mismo problema antes de identificar el problema
Cantidad de incidentes por problema conocido	▪ Cantidad promedio de incidentes vinculados al mismo problema después de identificar el problema
Tiempo hasta la identificación del problema	▪ Tiempo promedio transcurrido entre la primera aparición de un incidente y la identificación de la raíz

	del problema
Esfuerzo de resolución de problemas	▪ Tiempo promedio de esfuerzo de trabajo para resolver problemas.

KPI's ITIL - Perfeccionamiento Continuo del Servicio – CSI

- KPI's Evaluación de Servicios

KPI (Métrica de CSI)	Descripción
Cantidad de quejas de clientes	▪ Cantidad de quejas recibidas de los clientes
Cantidad de quejas de clientes aceptadas	▪ Cantidad de quejas recibidas de los clientes que fueron aceptadas como justificadas
Cantidad de encuestas de satisfacción de clientes	▪ Cantidad de encuestas de satisfacción de clientes formales realizadas durante el periodo del informe
Porcentaje de Cuestionarios Encuesta	▪ Porcentaje de cuestionarios encuesta, en relación a la cantidad total enviada
Cantidad de Evaluaciones de Servicios	▪ Cantidad de evaluaciones de servicios realizadas durante el periodo del informe
Cantidad de debilidades identificadas	▪ Cantidad de puntos débiles identificados durante la evaluación de servicio.

- KPI's Evaluación de Procesos

KPI (Métrica de CSI)	Descripción
Cantidad de Comparativas de Procesos, Evaluaciones de Madurez, y Auditorías	▪ Cantidad de comparativas de procesos formales, evaluaciones de madurez, y auditorías realizadas durante el periodo del informe
Cantidad de Evaluaciones de Procesos	▪ Cantidad de evaluaciones de procesos formales realizadas
Cantidad de debilidades identificadas	▪ Cantidad de puntos débiles identificados durante la evaluación de procesos, para ser tratados mediante iniciativas de mejoras

- KPI's Definición de Iniciativas de Mejoramiento

KPI	Descripción
Cantidad de Iniciativas	▪ Cantidad de iniciativas, resultado de los puntos débiles identificados durante la evaluación de servicios y procesos

Cantidad de Iniciativas completadas	▪ Cantidad de iniciativas que fueron completadas durante el periodo del informe

1.2.4 ISO/IEC 27002

Se enfoca al análisis de riesgo debido a que utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero.

Dentro del marco de la norma de seguridad ISO 27002 se tratara de identificar los siguientes elementos:

Por medio de entrevistas se busca entender los diferentes aspectos que conforman a la organización, tanto en el aspecto tecnológico, como en los procesos críticos.

Con la evaluación de riesgos se pretenden descubrir las amenazas, vulnerabilidades y riesgos de la información, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información, para posteriormente definir políticas y mecanismos.

El método o modelo que se empleará para el desarrollo del este escrito será el modelo de cascada, ya que éste ordena rigurosamente las etapas del ciclo de vida del sistema, de tal forma que el inicio de cada etapa debe esperar a la finalización de la inmediatamente anterior.

Las etapas son:

1. Análisis de requisitos. En esta fase se analizan las necesidades de los usuarios finales para determinar qué objetivos debe cubrir el sistema. Es importante señalar que en esta etapa se debe consensuar todo lo que se requiere del sistema y será aquello lo que seguirá en las siguientes etapas, no pudiéndose requerir nuevos resultados a mitad del proceso de elaboración del sistema.
2. Diseño del sistema. Se descompone y organiza el sistema o el problema en elementos que puedan elaborarse por separado, aprovechando las ventajas del desarrollo en equipo.
3. Elaboración del sistema. Se da marcha adelante en la elaboración del sistema contemplando los requisitos establecidos en la primera fase.
4. Pruebas. Los elementos se ensamblan para componer el sistema y se comprueba que funciona correctamente y que cumple con los requisitos, antes de ser implementado.
5. Implantación. El sistema se pone en producción. Durante la explotación del sistema pueden surgir cambios, bien para corregir errores o bien para introducir mejoras. Todo ello se debe de documentar.
6. Mantenimiento. Se le hacen actualizaciones al sistema, se modifica conforme lo requiere la dependencia.

De esta forma, cualquier error de diseño detectado en la etapa de prueba conduce necesariamente al rediseño y nueva programación del código afectado, mejorando así la seguridad al tomar en cuenta puntos vulnerables no vistos en un principio.

RESULTADO ESPERADO

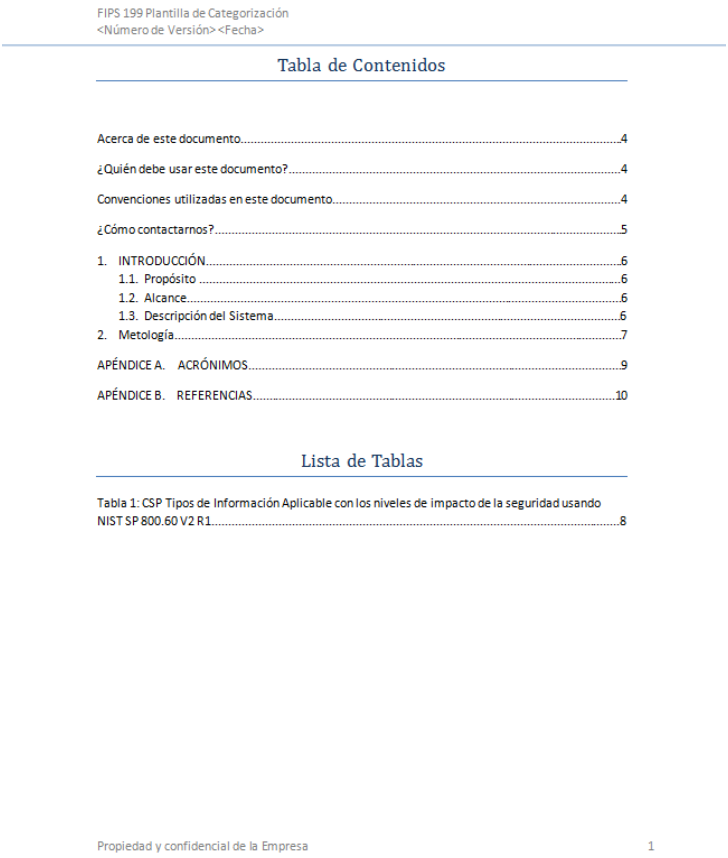
Al implementar la ISO 27002 se espera obtener lo siguiente:

- Garantizar los controles internos.
- Señalar que se respetan las leyes y normas de aplicación. Proporcionar una ventaja competitiva al cumplir los requisitos y demostrar a los usuarios que la seguridad de su información es primordial.
- Verificar que los riesgos de la organización estén correctamente identificados, evaluados y gestionados a la vez que se formalizan los procesos, procedimientos y documentación de protección de la información.
- Demostrar el compromiso con los Directivos de la organización y la seguridad de la información.
- Los procesos de evaluaciones periódicas ayudan a supervisar continuamente el rendimiento y la mejora.

1.2.5 FIPS PUB 200 (FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS)

La FIPS PUB 200 es una publicación relacionada con los Requerimientos Mínimos de Seguridad para Información Federal y Sistemas de Información (del inglés Minimum Security Requirements for Federal Information and Information Systems) desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST, del inglés National Institute of Standards and Technology) a petición de la Ley de Gestión de la Información Federal de 2002(FISMA, del inglés Federal Information Security Management Act of 2002).

Para cumplir con la norma federal, las organizaciones deben primero determinar la categoría de seguridad de su sistema de información, de acuerdo con FIPS 199, "Normas para la categorización de Seguridad de la Información y Sistemas de Información Federal", y luego aplicar la medida apropiada al conjunto de controles de seguridad con base en el NIST publicación Especial 800-53(Ilustración 4).



FIPS 199 Plantilla de Categorización
<Número de Versión> <Fecha>

Tabla de Contenidos

Lista de Tablas

Propiedad y confidencial de la Empresa 1

Ilustración 4. Plantilla del documento de FIPS PUB 200

Al aplicar las disposiciones de la FIPS PUB 200, las Organizaciones primero deben categorizar su sistema de información como es requerido por FIPS 199, y luego se selecciona un conjunto adecuado de controles de seguridad del NIST Special Publication 800-53 para satisfacer sus requerimientos de seguridad. Esto ayuda a asegurar que los requisitos y los controles de seguridad sean aplicables a toda la información federal y a los sistemas de información incluyendo la computación en la nube.

La evaluación organizacional de riesgo corrobora la selección de valores de control inicial y determina si los controles adicionales son necesarios para proteger:

- Las operaciones de la organización (incluyendo la misión, las funciones, la imagen o la reputación).
- Los activos de los procesos de la organización (los planes, las políticas, los procedimientos, los lineamientos, los cronogramas y datos sobre los riesgos).
- Las personas, otras organizaciones o la nación.

El resultado conjunto de los controles de seguridad acordados establece un nivel de la seguridad para la organización.[7]

Incluyen los siguientes procedimientos

- **Control de acceso**. Información sobre el límite de acceso al sistema a usuarios autorizados y de los tipos de transacciones y las funciones que los usuarios autorizados tienen permiso para ejercer.

- **Certificación, acreditación y evaluación de la seguridad**. Evaluar periódicamente los controles de seguridad, elaborar y aplicar planes de acción destinados a corregir las deficiencias y reducir las vulnerabilidades, autorizar el funcionamiento de los sistemas y las conexiones del sistema asociado y supervisar los controles de seguridad del sistema de forma continua.

- **Evaluación de riesgos**. Evaluar periódicamente el riesgo de las operaciones, activos y personas que resultan de la operación de los sistemas y el procesamiento asociado, almacenamiento o transmisión de la información.

Las organizaciones tienen la flexibilidad en la aplicación de los controles de seguridad de acuerdo con las orientaciones contenidas en el NIST Special Publication 800-53. Esto permite a las organizaciones seleccionar los controles de seguridad estrechamente alineados con la misión y los requerimientos del negocio y entornos de operación.

RESULTADO ESPERADO

- Esquemas para clasificar la información y los sistemas de información a nombre de agencias federales, sus objetivos son proporcionar los niveles adecuados de seguridad de la información de acuerdo con un rango de niveles de riesgo.

- Directrices para recomendar los tipos de sistemas de información y la información que se incluye en cada categoría.

- Los requisitos mínimos de seguridad de la información y sistemas de información para cada categoría.

1.2.6 ISO/IEC 13335 (GESTIÓN DE LA INFORMACIÓN DE LA TECNOLOGÍA DE LAS COMUNICACIONES Y SEGURIDAD)

La norma ISO/IEC 13335-1 es la primera que se ocupa de los aspectos de la planificación, implementación y operaciones, incluyendo el mantenimiento de la seguridad, mantenimiento de la información y comunicaciones que son una recopilación

[7] http://itlaw.wikia.com/wiki/FIPS_200

de 5 documentos que de forma práctica aborda la seguridad de las Tecnologías de la Información y orienta sobre los aspectos de su gestión. Estos documentos son:[8]

- Conceptos y modelos para la seguridad de las TI
- Gestión y planificación de la seguridad de las TI
- Técnicas para la gestión de la seguridad de las TI
- Selección de Protecciones
- Guía para la gestión de Seguridad en Redes

OBJETIVOS

Los Objetivos, estrategias y políticas deben ser formulados como una base para una seguridad efectiva dentro de una organización. Las normas que deben tomarse en cuenta en la implantación de las estrategias y los métodos de aplicación de las políticas se definen y desarrollan a través de diferentes niveles de una organización.

ASPECTOS ORGANIZACIONALES DE LA SEGURIDAD DE LAS TI

Los roles establecidos deberán tomar en cuenta el reconocimiento explícito de tareas dentro de la organización, el tamaño de la organización determinará el nivel de los compromisos que serán asignados.

FUNCIONES DE LA GESTIÓN DE LA SEGURIDAD DE LAS TI

El éxito de la seguridad y tecnologías de información requiere de una serie de actividades que se llevarán a cabo mediante un ciclo -Planificar -Implementar -Monitorizar –Actuar.

CICLO DE VIDA

Son fundamentales para la concepción y establecimiento de un sistema de seguridad de información y comunicaciones. En esta norma se describen los principales elementos y su relación de participación en los sistemas de seguridad, entre los cuales podemos nombrar:

- **Activos.** Pueden ser humanos, físicos, lógicos, intangibles.
- **Amenazas.** Ya sean humanas o ambientales.
- **Vulnerabilidad de los activos.** Riesgos potenciales a los activos.
- **Impacto.** Como resultante de un incidente de seguridad-riesgo-salvaguardas, de detección, limitación, detección, corrección.
- **Limitaciones.** Pueden ser: financieras, técnicas, sociológicas, personales, legales y de tiempo.

[8] http://es.scribd.com/doc/38930152/Resumen-Iso-Iec-13335

RESULTADO ESPERADO

El documento discute las definiciones clásicas de Seguridad de la Información y los riesgos de la información, nos muestra los principales procesos involucrados en la seguridad de la información como son: la gestión de la configuración, gestión del cambio, gestión del riesgo, análisis de riesgo y responsabilidad, concientización de seguridad, monitorizar, planificación de la contingencia y recuperación de desastres. También muestra diferentes modelos útiles para entender los elementos de seguridad definidos conceptualmente y la gestión de riesgo.

En resumen el documento define los conceptos necesarios para poder entender los elementos de la seguridad de la información y gestión de aspectos como lo son la planificación, implementación y operaciones incluyendo el mantenimiento de la seguridad, información y comunicaciones.

La ISO 13335 describe las estrategias para poner en práctica todos los procesos de seguridad, también menciona los diferentes roles y responsabilidades a nivel organizacional, así como un modelo de seguridad de la información amparado por la gobernabilidad de Tecnología de la Información o enfocado totalmente a los aspectos de tecnología de la información.[9]

1.2.7 ISO/IEC 15408:2005

Common Criteria for Information Technology Security Evaluation (abreviado como Common Criteria o CC) es una norma internacional (ISO / The *International Electrotechnical Commission* 15408) para la certificación de la seguridad del sistema. Actualmente se encuentra en la versión 3.1.

Common Criteria, es un marco en el que los usuarios del sistema informático pueden especificar su seguridad funcional y los requisitos de garantía, igualmente los vendedores pueden aplicar y/o hacer declaraciones sobre los atributos de seguridad de sus productos, y los laboratorios de ensayo puede evaluar los productos para determinar si, efectivamente, cumplen las reclamaciones. Common Criteria ofrece la garantía de que el proceso de especificación, implementación y evaluación de un producto de seguridad informática se ha realizado de forma rigurosa y cumpliendo estándares[10]

CONCEPTOS CLAVE AL MOMENTO DE EVALUAR EL SISTEMA

La evaluación sirve para validar las afirmaciones hechas sobre el objetivo. Para ser de uso práctico, la valoración debe verificar las características de seguridad del objetivo, esto se hace a través de los siguientes parámetros:

- **Objetivo de la evaluación**. Detecta la situación inicial para comenzar un proceso y el objetivo es poder elaborar informes descriptivos del mismo.

[9] http://gestionsegura.blogspot.mx/2007/06/iso-13335-gua-para-la-gestin-de.html
[10] http://www.sans.org/reading_room/whitepapers/standards/common-criteria-iso-iec-15408-insight-thoughts-questions-issues_545

- **Perfil de protección**. define un conjunto de objetivos y requisitos de seguridad, independiente de la implantación, que cubre las necesidades de seguridad comunes de los usuarios.

- **Objetivo de Seguridad**. Herramienta útil ya que permite definir especificaciones de seguridad independientes de implementación, que pueden ser utilizadas como base de especificaciones para productos o sistemas.

- **Requisitos de seguridad funcional.** Estos proporcionan mecanismos para hacer cumplir las políticas de seguridad.

- **Garantía de los Requisitos de Seguridad.** Proporcionan la base para la confianza en que un producto verifica sus objetivos de seguridad.

- **Nivel del Garantía de la Evaluación**. Proporcionan una escala incremental que equilibra el nivel de confianza obtenido con el coste y la viabilidad de adquisición de ese grado de confianza

1.2.8 PRINCE 2 (PROJECTS IN A CONTROLLED ENVIRONMENT)

En español Proyectos en un Entorno Controlado, es un método para la administración de proyectos en especial para la organización, la gestión y el control, utilizado en el Reino Unido, es ampliamente reconocido y utilizado en el sector privado.

Este método divide los proyectos en fases para poder controlar los recursos y la evolución del mismo.

PRINCE2 ofrece una serie de procesos que explican qué debe ocurrir y cuándo dentro del proyecto.

Cualquier proyecto guiado con este método debe incorporar estos procesos en alguna forma, pero lo más importante, es ajustar el Modelo de Procesos a los requisitos del proyecto en el que estemos trabajando, tenemos que enfocar la gestión preguntándonos hasta qué punto debe ser aplicado cada proceso a cada proyecto.

La estructura de Prince2 está organizada en tres partes:

1. **Componentes**. Son las áreas de conocimiento que deben aplicarse al proyecto cuando correspondan.

2. **Procesos**. Estos ayudan a implementar los componentes, indican qué debe ocurrir y cuándo a lo largo del ciclo de vida del proyecto.

3. **Técnicas**. Son métodos de trabajo opcionales.

Prince2 define 8 componentes, 8 procesos y 3 técnicas para la versión 2005; para la versión 2009 a los componentes se les denomina temas y se definen 7 temas, 7 procesos

y 2 técnicas además de 8 roles contra 10 que se tenían con la versión 2005.[11](Ilustración 5).

	Versión	
	2005	2009
Componentes	1. Proceso de Negocio 2. Organización 3. Planes 4. Controles 5. Riesgo 6. Calidad 7. Gestión de Configuración 8. Control del Cambio	1. Proceso de Negocio 2. Organización 3. Calidad 4. Planes 5. Riesgo 6. Control del Cambio 7. Progreso
Procesos	1. [SU] Comienzo de un Proyecto 2. [IP] Inicio de un Proyecto 3. [DP] Dirigir un Proyecto 4. [CS] Controlar una Fase 5. [MP] Gestión del Suministro de Productos 6. [SB] Gestión del Límite de las Fases 7. [CP] Cerrar un Proyecto 8. [PL] Planificación	1. [SU] Comienzo de un Proyecto 2. [IP] Inicio de un Proyecto 3. [DP] Dirigir un Proyecto 4. [CS] Controlar una Fase 5. [MP] Gestión del Suministro de Productos 6. [SB] Gestión del Límite de las Fases 7. [CP] Cerrar un Proyecto
Técnicas	1. Planificación en Base del Producto 2. Control del Cambio 3. Revisión de la Calidad	1. Planificación en Base del Producto 2. Revisión de la Calidad
Roles	1. Consejo/Junta Directiva 2. Usuario Representativo 3. Director Ejecutivo 4. Suministrador/Proveedor Representativo 5. Jefe de Proyecto 6. Jefe de equipo 7. Responsable de Garantía 8. Responsable de Soporte 9. Bibliotecario de la Configuración 10. Oficina de Soporte de Proyecto	1. Consejo/Junta Directiva 2. Usuario Representativo 3. Director Ejecutivo 4. Suministrador/Proveedor Representativo 5. Jefe de Proyecto 6. Jefe de Equipo 7. Responsable de la Garantía 8. Responsable de Soporte

Ilustración 5 Comparación de versiones de Prince2

[11] http://www.liderdeproyecto.com/articulos/introduciendo_a_prince2.html

RESULTADO ESPERADO

Existen dos maneras de acreditarse como practicante de PRINCE2 y es mediante los cursos de PRINCE2 Foundation y Practitioner Syllabus.

En el primer curso se da una introducción a PRINCE2 y se aprenden los conceptos básicos y terminología del método, se debe demostrar que el practicante es capaz de describir el propósito y contenido principal de los principios, temas y procesos. Así mismo, cuáles son los productos de entrada, salida y relaciones entre los procesos, los resultados, roles y dimensiones de la gestión de un proyecto. Se realiza un examen que es de opción múltiple y dura una hora y consta de 75 preguntas que deben ser contestadas a libro cerrado y de las cuales se debe tener al menos 38 preguntas contestadas correctamente para acreditar.

El segundo curso tiene por objetivo medir cómo el candidato:

- Puede aplicar PRINCE2 para el correcto funcionamiento y gestión de un proyecto dentro de un ambiente de apoyo.

- Tiene la competencia necesaria para aplicar y ajustar las necesidades de un proyecto específico.

- Es capaz de explicar detalladamente todos los principios, temas, conjunto de actividades o eventos y ejemplos prácticos de todos los productos de PRINCE2.

- Explicar las relaciones entre estos y las razones detrás de estos principios.

- Aplicar esta comprensión a diferentes circunstancias del proyecto.

El examen consta de 9 preguntas que valen 12 puntos cada una con una duración de 2.5 horas a libro cerrado y es necesario obtener una puntuación de 59 de un total de 108 preguntas para acreditar.

Cualquier proyecto que utilice este método debe incorporar los siguientes procesos en alguna forma, obviamente lo más importante es ajustar el Modelo de Procesos a los requisitos del proyecto en el que se esté trabajando. (Ilustración 6)

- **Dirección de un Proyecto** (DP, del inglés Directing a Project). Este proceso es para la Gestión Superior, es decir, la Junta de Proyecto que se encarga de controlar el proyecto.

- **Puesta en Marcha de un Proyecto** (SU, del inglés Starting Up a Project). Se refiere a un proceso de pre-proyecto muy corto que reúne los datos necesarios para comenzar el proyecto.

- **Iniciar un Proyecto** (IP, del inglés Initiating a Project). Su objetivo es examinar la justificación del plan y crear la Documentación de Inicio del Proyecto (PID) que incluye el Plan del Proyecto (Project Plan).

- **Control de una Fase** (CS Controlling a Stage). Describe las tareas diarias de vigilancia y de inspección que realiza el Jefe de Proyecto sobre el Proyecto.

- **Gestión de los Límites de Fase** (SB, del inglés Managing a Stage Boundary). Se encarga de proporcionar una forma controlada de completar una fase y planear la siguiente.

- **Gestión de la Entrega de Productos** (MP Managing Product Delivery). Es donde los productos que van a ser utilizados por los usuarios, son entregados por los miembros del equipo.

- **Cerrar un proyecto** (CP, del inglés Closing a Project). Se encarga de confirmar la entrega de los productos y el Jefe de Proyecto prepara el cierre del proyecto.

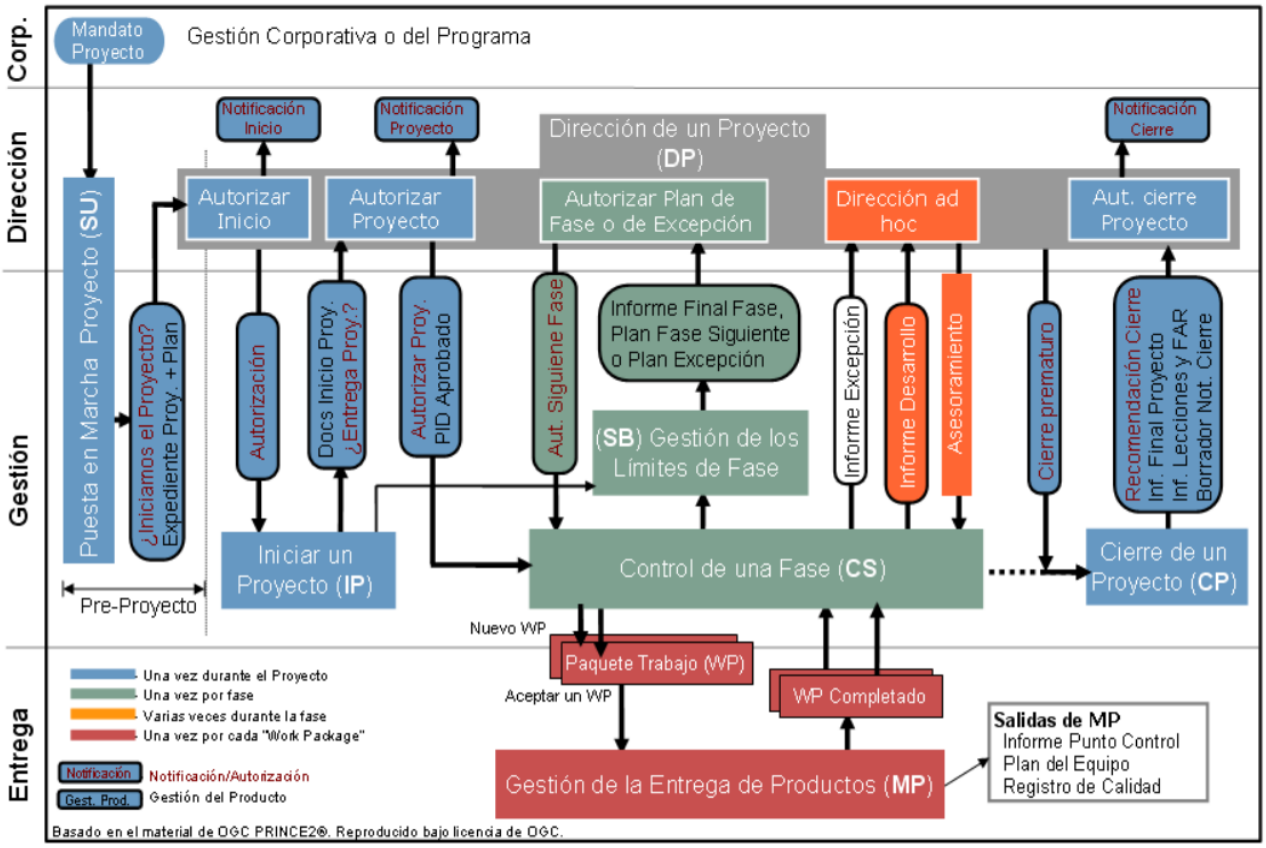


Ilustración 6. Modelo de Procesos PRINCE2.

1.2.9 PMBOOK(PROJECT MANAGEMENT BODY OF KNOWLEDGE)

Es un estándar para dirigir proyectos en diversos tipos de industrias, desarrollado por Project Management Institute (PMI). Describe cuáles son los procesos, herramientas y técnicas para la gestión de proyectos, establece 5 grupos de procesos básicos y 9 áreas de conocimiento comunes a todos los proyectos. (Ilustración 7)

Grupos básicos de procesos:

1. **Iniciación**. Se define un proyecto o una nueva fase de un proyecto existente.

2. **Planificación**. Define, refina los objetivos y planifica el curso de acción requerido para lograr los objetivos y el alcance pretendido del proyecto. Está formado por veinte procesos

3. **Ejecución**. Compuesto por aquellos procesos realizados para completar el trabajo definido en el plan a fin de cumplir con las especificaciones del mismo. Implica coordinar personas y recursos, así como integrar y realizar actividades del proyecto en conformidad con el plan para la dirección del proyecto.

4. **Seguimiento y control**. Mide, supervisa y regula el progreso y desempeño del proyecto, para identificar áreas en las que el plan requiera cambios

5. **Cierre**. Formaliza la aceptación del producto, servicio o resultado, y termina ordenadamente el proyecto o una fase del mismo

	Grupo de Procesos de Iniciación	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupo de Procesos de Seguimiento y Control	Grupo de Procesos de Cierre
1. Gestión de la Integración del Proyecto	1.1 Desarrollar el Acta de Constitución del Proyecto	1.2 Desarrollar el Plan para la Dirección del Proyecto	1.3 Dirigir y Gestionar la ejecución del Proyecto	1.4 Monitorizar y Controlar el trabajo del Proyecto 1.5 Realizar el Control Integrado de Cambios	1.6 Cerrar Proyecto o Fase
2. Gestión del Alcance del Proyecto		2.1 Recopilar requisitos 2.2 Definir el Alcance 2.3 Crear EDT		2.4 Verificar el Alcance 2.5 Controlar el Alcance	
3. Gestión del Tiempo del Proyecto		3.1 Definir las actividades 3.2 Secuenciar las actividades 3.3 Estimar los Recursos de las Actividades 3.4 Estimar la Duración de las Actividades 3.5 Desarrollar el Cronograma		3.6 Controlar el Cronograma	
4. Gestión de los Costos del Proyecto		4.1 Estimar los Costos 4.2 Determinar el Presupuesto		4.3 Controlar los Costos	
5. Gestión de la Calidad del Proyecto		5.1 Planificar la Calidad	5.2 Realizar el Aseguramiento de Calidad	5.3 Realizar el Control de Calidad	
6. Gestión de los Recursos Humanos del Proyecto		6.1 Desarrollar el Plan de Recursos Humanos	6.2 Adquirir el Equipo del Proyecto 6.3 Desarrollar el Equipo del Proyecto 6.4 Dirigir el Equipo del Proyecto		
7. Gestión de las Comunicaciones del Proyecto	7.1 Identificar a los Interesados (Stakeholders)	7.2 Planificar las Comunicaciones	7.3 Distribuir la Información 7.4 Gestionar las expectativas de los interesados	7.5 Informar el Desempeño	
8. Gestión de los Riesgos del Proyecto		8.1 Planificar la Gestión de Riesgos 8.2 Identificar los Riesgos 8.3 Realizar el Análisis Cualitativo de Riesgos 8.4 Realizar el Análisis Cuantitativo de Riesgos 8.5 Planificar la Respuesta a los riesgos		8.6 Monitorizar y Controlar los Riesgos	
9. Gestión de las Adquisiciones del Proyecto		9.1 Planificar las Adquisiciones	9.2 Efectuar las Adquisiciones	9.3 Administrar las Adquisiciones	9.4 Cerrar las Adquisiciones

Ilustración 7. Áreas de conomiento y procesos.

La organización debe cumplir los siguientes niveles:

- **Nivel I. Alcanzar los objetivos del proyecto**

  Tener la certeza documentada de que los objetivos del proyecto se han cumplido**.**

- **Nivel II. Eficiencia del proyecto**.

  Para medir la eficiencia se debe tomar en cuenta los siguientes aspectos:

  - Nivel de interrupción del trabajo del cliente.
  - Eficiencia en el uso de los recursos
  - Crecimiento del número de miembros del equipo
  - Gestión de conflictos

- **Nivel III. Utilidad para el usuario/cliente final**.

  Saber el nivel de utilidad sobre el usuario es muy importante para saber si se ha cumplido con los objetivos del proyecto y esto se puede saber si:

  - Se ha solucionado el problema inicial
  - Se han incrementado los beneficios
  - El usuario actualmente usa el producto

- **Nivel IV. Mejora organizacional**

  Aprender sobre la experiencia

JEFE DE PROYECTO

Se debe contar con un Jefe de Proyecto que tendrá las siguientes responsabilidades:

- El proyecto.
  - Objetivos de determinación de costos.
  - Calendario.
  - Funcionalidad.
  - Calidad.
  - Organización.
  - Retorno de la inversión.
- Flujo de información. Proporcionarla de forma proactiva.

- El equipo. Proporcionar realimentación y reconocimiento.
- Sobre él mismo. Crecimiento personal.
- Gestión del proyecto: Herramientas para la planificación y monitorización.
- Relaciones interpersonales
    - Capacidad de liderazgo, negociación y delegación.
    - Capacidad comunicativa oral y escrita.
    - Resolución de conflictos.
    - Habilidades para desarrollar el rol de mentor.
- Conocimiento tecnológico
    - Conocimiento de la industria y de las áreas tecnológicas
    - Conocimiento del producto y/o procesos
    - Habilidades de diseño
- Habilidades personales
    - Honestidad, integridad
    - Pensar simultáneamente
    - Alta tolerancia a la incertidumbre y a la ambigüedad
    - Persuasivo y asertivo
    - Abierto y accesible
    - Decisivo
    - Comercial. Capacidad para vender ideas o las propias virtudes del proyecto.
    - Profesor. Transmitir conocimiento a los miembros del equipo.

DEFINICIÓN DEL PROYECTO

La definición del proyecto se encuentra constituida por las siguientes fases:

- **Fase I.** Entender el problema o la oportunidad que se presenta.
- **Fase II**. Identificar la solución óptima.
- **Fase III.** Desarrollar una solución y proceder a la elaboración de un plan.
- **Fase IV.** Lanzamiento del proyecto.

FASE I. ENTENDER EL PROBLEMA O LA OPORTUNIDAD.

Es fundamental identificar la necesidad real que el proyecto pretende cubrir. El trabajo se evaluará en función de si esta necesidad ha sido cubierta satisfactoriamente o no.

En primer lugar se requiere diferenciar entre necesidad y solución. Una necesidad:

- Describe el fin para el cliente.
- Especifica metas y objetivos.
- Deja abierta la pregunta de ¿Cómo hacerlo?
- La respuesta al por qué se está haciendo debe apuntar a una justificación de negocio.

En cambio, una solución:

- Describe los medios para el equipo.
- Especifica estrategias e ideas para conseguir las metas y objetivos.
- Especifica cómo hacerlo.
- La respuesta al por qué se está haciendo debe apuntar al requerimiento del cliente.
- Preguntar para identificar la necesidad real puede hacer sentir incómodos a terceros por desconfiar de su criterio.

Con base en estas definiciones, esta fase debe tener un documento de salida con los requerimientos del proyecto, el cual no ofrece una solución sino que únicamente describe una necesidad. Este documento debe contener los siguientes apartados:

- Descripción del problema u oportunidad
- Impacto o efecto del problema
- Identificar quién o qué se encuentra afectado por el problema
- Cuál es el impacto al ignorar el problema
- Situación deseada
- Beneficios asociados al conseguir la situación deseada
- Alineación con la estrategia de la organización
- Conflicto de compatibilidades con otras áreas de la organización
- Incertidumbres
- Suposiciones clave

- Limitaciones de la solución
- Consideraciones del entorno
- Información histórica de soporte

A partir de la recopilación de toda esta información, se requiere valorar nuevamente si es suficiente para resolver el problema y determinar si existe una solución potencial.

FASE II. IDENTIFICAR LA SOLUCIÓN ÓPTIMA

Con objeto de identificar soluciones que cubran la necesidad establecida se puede seguir el siguiente procedimiento:

- Realizar una lluvia de ideas grupal con miembros del futuro equipo de trabajo o las partes involucradas.
- Comprobar en qué grado satisfacen los planteamientos del documento de requerimientos del proyecto.
- Seleccionar entre 2 y 5 soluciones candidatas.

Para las soluciones candidatas seleccionadas conviene realizar un análisis detallado para identificar cuál de ellas es la que mejor se adapta a la necesidad a cubrir e implica un costo asumible.

ANÁLISIS FINANCIERO (COSTOS VS BENEFICIOS)

Para validar la viabilidad financiera del proyecto es necesario identificar los flujos de entrada de dinero que este puede generar, por ejemplo: beneficios obtenidos por la implementación del proyecto (incremento en ventas, reducción en costos) y los gastos que representa la puesta en marcha y gestión del proyecto.

FASE III. DESARROLLO DE LA SOLUCIÓN Y ELABORACIÓN DE UN PLAN

En esta fase se desarrollará en un mayor detalle la solución elegida mediante el uso de un esquema básico de definición del proyecto.

El esquema básico de definición del proyecto se encuentra dividido en varios niveles:

- Objetivo
- Propósito
- Resultados
- Actividades

Para cada uno de estos niveles se deben especificar:

- Indicadores que permitan verificar la evolución.
- Medios para obtener la información necesaria para constituir los indicadores.
- Supuestos clave y el riesgo asociado.

FASE IV. LANZAMIENTO DEL PROYECTO

Antes de realizar el lanzamiento, es importante verificar que dispondremos de todos los recursos necesarios. Una vez confirmado este aspecto, se requieren dos pasos:

1. Obtener la aprobación definitiva de la dirección
2. Reunir al equipo de trabajo seleccionado para informarles del proyecto en el que van a participar.

De cara a la aprobación por la dirección, es recomendable la elaboración de un documento de propuesta que contenga los siguientes apartados:

- Breve descripción de las necesidades
- Acciones recomendadas
- Beneficios
- Riesgos a asumir si se lleva a cabo la acción
- Riesgos a asumir si no se realiza alguna acción
- Costos y ahorros (estimaciones en rangos de valores)
- Calendario
- Métricas (como se medirá el resultado para valorar el éxito)
- Incertidumbres
- Suposiciones
- Limitaciones
- Apoyo requerido
- Listado de organizaciones que deben involucrarse y en qué medida
- Impacto en el resto de la organización
- Grado de apoyo activo por parte de la dirección.
- Factores críticos para el éxito.

Por otra parte, la reunión inicial con el equipo de trabajo debe encontrarse dirigida hacia los siguientes objetivos:

- Reconocer la formación oficial del equipo.
- Indicar cuáles son las expectativas.
- Promover la cohesión del grupo.

CONSTRUIR Y MANTENER UN EQUIPO EFECTIVO.

El equipo de trabajo, es una de las partes claves del proyecto. Antes de iniciar el trabajo, conviene anticiparse a las preguntas y ansiedades del equipo:

- ¿Me conviene el proyecto?
- ¿Qué se espera de mí?
- ¿Cómo será el trabajo en equipo?

Cada equipo es un mundo y su evolución depende en gran parte de las capacidades y experiencias de los miembros del mismo. No obstante, en términos generales se podrían listar las siguientes fases evolutivas:

- **Formación**
    - Los miembros del equipo requieren adquirir conocimientos sobre el proyecto y comprobar su relación con el resto.
    - El jefe de proyecto debe organizar y proveer la máxima información.
- **Reacción**
    - Con base en lo aprendido, los miembros del equipo valoran los objetivos, roles y relaciones establecidas. Puede dar lugar a conflictos.
    - El jefe de proyecto debe guiar e intentar llegar a soluciones pactadas para los conflictos generados.
- **Normalización**
    - Si se superan los posibles conflictos de la etapa anterior, se pasa a la normalización mediante la creación de normas de conducta.
    - El jefe de proyecto debe animar a cada uno de los miembros a participar más activamente. Potenciar la sensación de propiedad por parte de los miembros hacia sus objetivos y tareas.
- **Acción**
    - El equipo funciona con un buen grado de autonomía, produciendo resultados de calidad.
    - El jefe de proyecto debe ser un facilitador del flujo de trabajo

RESULTADO ESPERADO

- Identificar el problema o la oportunidad
- Identificar y definir la solución idónea
- Identificar las tareas y los recursos necesarios.
- Preparar el calendario y la obtención de recursos
- Estimar el costo del proyecto y preparar un presupuesto
- Analizar los riesgos y establecer relaciones que toda persona que tenga un interés directo o indirecto en el proyecto: Gestión del riesgo periódico.
- Mantener el control y la comunicación en el nivel adecuado durante la ejecución: Reuniones periódicas para detectar y comunicar desviaciones.
- Gestionar un cierre satisfactorio
    - Listado de tareas para poder acabar el proyecto.
    - Los miembros del equipo tienden a dispersarse dado que el proyecto se encuentra casi cerrado.[12]

1.2.10 TICKIT

Es un esquema de certificación para la administración de calidad del software, es utilizado en Reino Unido y Suecia, en general permite que desarrolladores de software y proveedores alcancen sus objetivos de acuerdo con lo que dicta lo norma ISO 9001 referida a gestión de calidad.

Esta herramienta, crea un marco metódico para que las organizaciones se encaminen a la mejora continua y acrecentando su competitividad.

La Guía TickIT se compone de 6 partes (Ilustración 8):

- **Pieza A**: Introducción a TickIT y el proceso de certificación, en esta fase describe de manera general como opera TickIT y se relaciona con otras iniciativas como la mejora de proceso.
- **Pieza B**: Guía a los clientes y explica cómo pueden contribuir a la calidad de los productos y servicios entregados.
- **Pieza C**: Guía a las Organizaciones y a sus proveedores en la construcción de un sistema de gestión de la calidad usando los procedimientos de TickIT.

[12] http://www.marblestation.com/?p=660

- **Parte D**: Guía a los auditores sobre cómo usar los procedimientos de TickIT.

- **Parte E**: Requerimientos del sistema de gestión de calidad del software siguiendo las cláusulas del estándar e interpretando los requisitos de manera adecuada del ISO 9001:2000.

- **Parte F**: Requisitos del sistema de gestión de calidad del software desde la perspectiva de procesos básicos requeridos para el desarrollo, mantenimiento y ayuda del software y siguiendo la norma ISO/IEC 12207:1995.

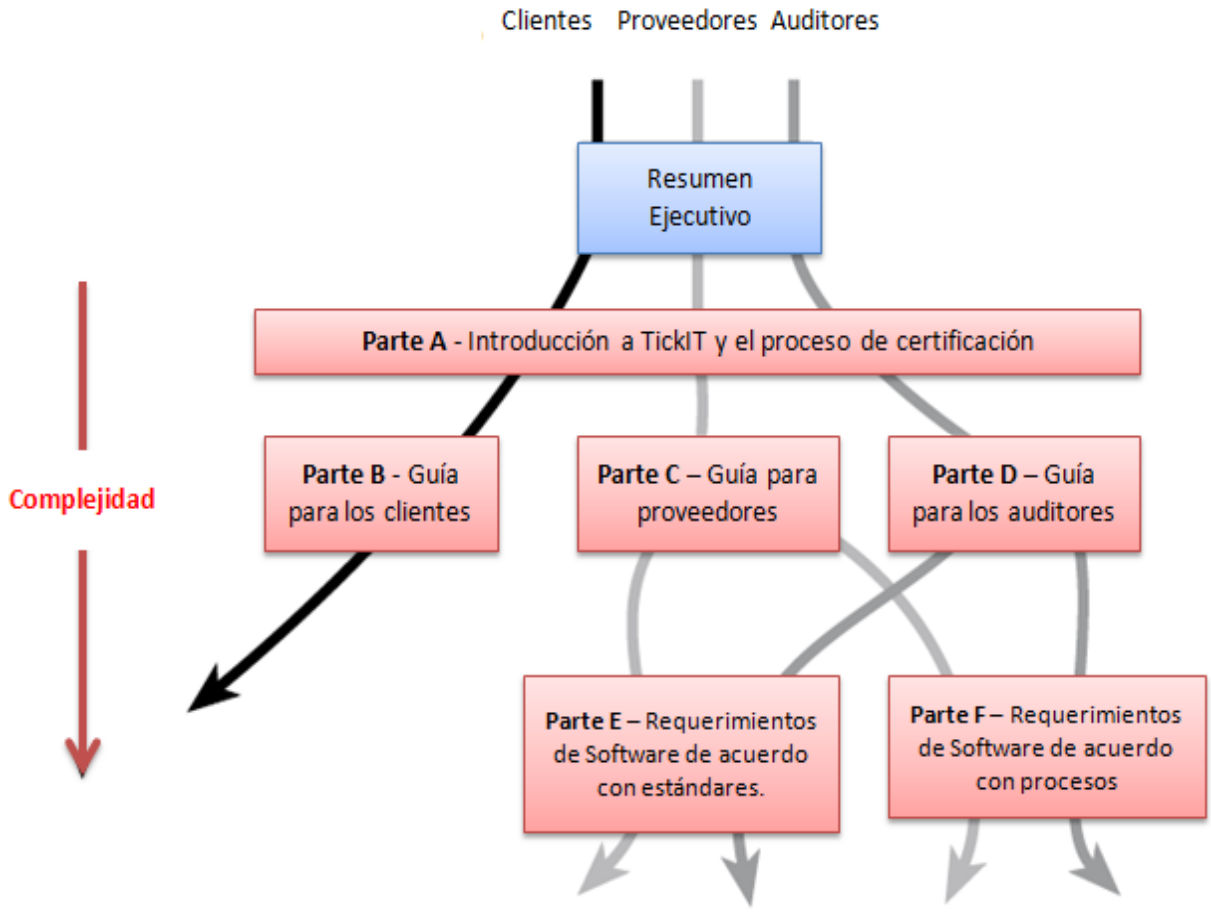


Ilustración 8. Maneras de uso de TickIT

RESULTADO ESPERADO

Lo que se espera al implementar TickIT es lo siguiente:

- Mejorar la confianza del mercado mediante una certificación de calidad del sistema de gestión a través de los organismos de certificación acreditados para el sector de software.

- Mejorar la práctica profesional entre los auditores de sistemas de gestión de calidad en el sector del software.

- Publicar una guía autorizada para todos los interesados.
- TickIT utiliza ISO 9001:2000 esto implica tener una excelente base para garantizar la calidad del diseño, desarrollo, producción, instalación y servicio del software al grado de compararlo con el estándar con el cual se evalúan los sistemas de gestión de calidad para el software.

1.2.11 CMMI(CAPABILITY MATURITY MODEL INTEGRATION)

CMMI (en español Integración de modelos de madurez de capacidades) se trata de un conjunto de cuatro modelos elaborados por el Instituto de Ingeniería del Software (SEI) de los Estados Unidos, los cuales permiten evaluar la madurez en los procesos en una organización y describir las tareas que se deben llevar a cabo para mejorar dichos procesos.

De los cuatro modelos CMMI la organización elige el que más se ajusta a sus necesidades, los modelos son los siguientes:

1. **SS-CMM**. Provisión Externa
2. **IPPD-CMM**. Desarrollo Integrado de Producto y Proceso
3. **SE-CMM.** Ingeniería de Sistemas
4. **SW-CMM**. Ingeniería del Software

SE-CMM y SW-CMM en la nueva versión que se conoce como CMMI son remplazados por el título CMMI para desarrollo.

Para cada área de proceso se define una serie de buenas prácticas, como lo es: describir y documentar un procedimiento; proveer la información necesaria; ejecutar de un modo sistemático, universal y uniforme; y, contar con medidas que estén verificadas.

CMMI cuenta con dos representaciones diferentes: continua y por etapas.

La representación continua permite elegir un área de proceso o grupo de áreas de proceso y mejorar los procesos que se relacionan con esta. En esta representación se utilizan seis niveles de capacidad para identificar la mejora de un área de proceso individual.

Los niveles de capacidad, son los siguientes:

0. **Incompleto**. El proceso no se realiza o no se consiguen los objetivos.
1. **Ejecutado**. El proceso es ejecutado y cumple los objetivos.

2. **Gestionado**. El proceso es ejecutado, además se planifica de acuerdo con políticas, se monitoriza, se controla, se revisa y se evalúa el proceso.

3. **Definido**. El proceso es gestionado, estableciendo el propósito, las entradas, los criterios de entrada, las actividades, los roles, las medidas, las etapas de verificación, las salidas y los criterios de salida. Se ajusta a la política de procesos dentro de la organización.

4. **Cuantitativamente gestionado**. Este proceso se controla utilizando técnicas estadísticas y otras técnicas cuantitativas, tomando en cuenta la calidad y rendimiento del proceso.

5. **En optimización**. El proceso se enfoca en una mejora continua, se revisa y modifica para adaptarlo a los objetivos del negocio.

La representación por etapas emplea conjuntos predefinidos de áreas de proceso y especifica un camino de mejora el cual se describe por niveles de madurez.

Los cinco niveles de madurez son los siguientes:

1. **Inicial**. Los procesos no son estables, exceden el presupuesto y no cumplen calendarios.

2. **Gestionado**. Los procesos se planifican, realizan y gestionan de acuerdo a planes documentados.

3. **Definido**. Los procesos se gestionan constantemente manejando las interrelaciones entre las actividades del proceso y las medidas detalladas del proceso, los productos de trabajo y sus servicios.

4. **Gestionado cuantitativamente**. El producto de los procesos se controla utilizando técnicas estadísticas y otras técnicas cuantitativas.

5. **En optimización**. El proceso se mejora continuamente, los efectos de las mejoras se miden y evalúan de acuerdo con los objetivos cuantitativos de mejora del proceso.

La elección de alguna de las dos representaciones depende de la organización y el conocimiento que se tiene de los procesos que necesitan ser mejorados.

Si se ha detectado qué procesos requieren ser optimizados y sus respectivas dependencias de las áreas en CMMI la representación continua es la opción a elegir. En cambio, si no se tiene idea de por dónde empezar ni qué procesos elegir para su mejora, la representación por etapas es la indicada.

RESULTADO ESPERADO

Para evaluar a las organizaciones que ocupan CMMI se utiliza el método SCAMPI (del inglés Standard CMMI Appraisal Method for Process Improvement), el cual da como resultado una calificación.

Para la representación continua la calificación es un perfil del nivel de capacidad el cual consta de una lista de áreas de procesos con el respectivo nivel de capacidad alcanzado. En cambio en una representación por etapas la calificación es un nivel de madurez, se aporta la serie de perfiles objetivo que tiene su equivalente a un nivel de madurez de la representación.

SCAMPI incluye los métodos de evaluación de Clase A, B y C.

- **SCAMPI A.** Es el método más riguroso y el único método que puede dar lugar a una calificación.
- **SCAMPI B.** Proporciona opciones en el alcance del modelo, pero la caracterización de las prácticas está fijada en una escala y se realiza sobre prácticas ya implementadas.
- **SCAMPI C.** Ofrece un amplio rango de opciones, incluyendo la caracterización de enfoques planificados para la implementación de procesos de acuerdo con una escala definida por el usuario.[13]

SCAMPI es una serie de cuestionarios para cada una de las áreas de proceso de CMMI, las cuales son 22:

1. Análisis causal y resolución (CAR, del inglés Causal Analysis and Resolution).
2. Análisis de decisiones y resolución (DAR, del inglés Decision Analysis and Resolution).
3. Aseguramiento de la calidad de proceso y de producto (PPQA, del inglés Process and Product Quality Assurance).
4. Definición de procesos de la organización + IPPD1 (OPD + IPPD, del inglés Organizational Processes Defining).
5. Desarrollo de requerimientos (RD, del inglés Requirements Development).
6. Enfoque en procesos de la organización (OPF, del inglés Organizational Processes Focus).
7. Formación organizativa (OT, del inglés Organizational Training).
8. Gestión cuantitativa de proyecto (QPM, del inglés Quantitative Project Management).
9. Gestión de acuerdos con proveedores (SAM, del inglés Supplier Agreement Management).
10. Gestión de configuración (CM, del inglés Configuration Management).

[13] CHRISSIS, Mary Beth, et al. "CMMI, Guía para la integración de procesos y la mejora de productos". 2ª. Ed. Pearson Educación. México: 2009. Pág.109

11. Gestión de requerimientos (REQM, del inglés Requirements Management).
12. Gestión de riesgos (RSKM, del inglés Risk Management).
13. Gestión integrada del proyecto + IPPD1 (IPM + IPPD).
14. Innovación y despliegue en la organización (OID, del inglés Organization, Innovation and Deployment).
15. Integración de producto (PI, del inglés Product Integration).
16. Medición y análisis (MA, del inglés Measure and Analysis).
17. Monitorización y control del proyecto (PMC, del inglés Project Monitoring and Control).
18. Planificación de proyecto (PP, del inglés Project Planing).
19. Rendimiento del proceso de la organización (OPP).
20. Solución técnica (TS, del inglés Technical Solution).
21. Validación.
22. Verificación.

En esta plantilla que proporciona SCAMPI (Ilustración 9) se ingresan las calificaciones que obtuvieron los representantes por cada área de proceso y se mostrarán los resultados para su análisis, utilizando gráficas radiales. Cada pregunta se califica de acuerdo con la siguiente escala de puntuación:

- **0 – 1**. Esta práctica no se requiere y casi nunca se realiza.
- **2 – 3**. Esta práctica a veces se requiere y a veces se realiza.
- **4 – 5.** Esta práctica es requerida pero no siempre se realiza o la práctica es regularmente realizada aunque no es requerida o supervisada.
- **6 – 7**. Esta práctica es normalmente requerida y usualmente realizada.
- **8 – 9**. Esta práctica es requerida, es realizada y es supervisada.
- **10**. Esta práctica está institucionalizada y es un ejemplo de clase mundial.
- **?**. Si el participante no conoce la respuesta.
- **NA**. Si la práctica no es aplicable.

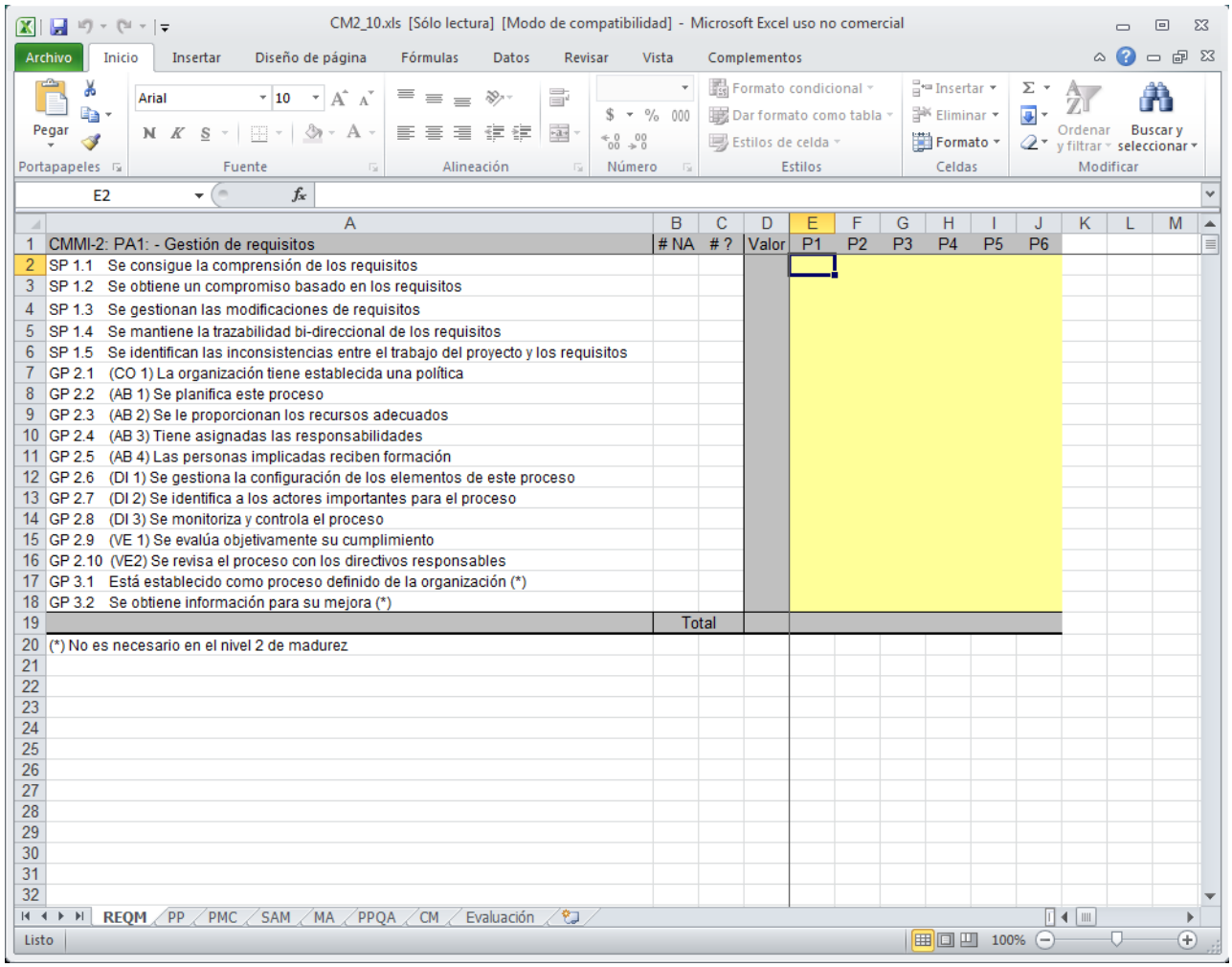


Ilustración 9. Plantilla para evaluación de niveles de CMMI.

1.2.12 TOGAF(THE OPEN GROUP ARCHITECTURE FRAMEWORK)

En español significa Esquema de Arquitectura de Grupo Abierto, es un marco de trabajo de arquitectura empresarial el cual se enfoca en el diseño, planificación, implementación y gobierno de la arquitectura empresarial de la información.

Cuenta con cuatro niveles o dimensiones:

1. **Arquitectura de Negocios o Procesos de Negocio**. En esta fase se definen estrategias del negocio, la manejabilidad, la estructura y los procesos clave de la organización.

2. **Arquitectura de Aplicaciones**. Se refiere a la representación para cada sistema de aplicación que se debe implantar y a cómo interactúan los sistemas y su relación con los procesos del negocio en la organización.

3. **Arquitectura de Datos**. Se refiere a la estructura de los datos físicos y lógicos en la organización y con qué recursos se cuenta para administrar estos datos.

4. **Arquitectura Tecnológica**. Se enfoca a la estructura de hardware, software y redes necesarias para implementar las aplicaciones requeridas en la organización.

Los principales componentes de TOGAF son:

- **ADM (Architecture Development Method)**. Es un método que se encarga de que se cumpla con las necesidades de la organización y de las TIC's. Describe para cada fase los objetivos, el enfoque, las entradas, las fases y las salidas. Proporciona resúmenes para administrar el cumplimiento de los requisitos.

- **Guías y Técnicas para ADM**. Son guías y técnicas que se adaptan a diferentes contextos dependiendo del proceso.

- **Framework del contenido de la arquitectura**. Proporciona una guía detallada de los productos que produce la arquitectura mediante entregables.

- **Enterprise Continumm y Herramientas**. Proporciona métodos para clasificar los artefactos de la solución y la arquitectura mostrando cómo se relacionan y pueden ser usados. Se basa en patrones, modelos y descripciones arquitectónicas que ya existen en la organización.

- **Modelos de Referencia**

    - **TRM (Technical Reference Model).** Es un catálogo o clasificación de los servicios genéricos de la plataforma.

    - **III-RM (Integrated Information Infrastructure Model).** Enfocado a las aplicaciones de negocios e infraestructura.

- **Framework de la capacidad de la arquitectura**. Son un conjunto de recursos, guías, plantillas, roles y responsabilidades que ayudan al arquitecto a establecer y operar una arquitectura empresarial.

Los productos de TOGAF, se agrupan en 3 categorías:

1. **Entregable**. Es el producto de trabajo que está definido y que es revisado, acordado y firmado por los interesados. La unión de estos entregables forma un proyecto.

2. **Artefacto**. Es un producto de trabajo más minucioso que describe una arquitectura desde un punto de vista. Ejemplos: diagrama de red, especificación de un servidor, especificación de un caso de uso y se subdivide en:

    - Catálogos (listas de elementos).

    - Matrices (relaciones entre elementos).

- Diagramas (dibujos de los elementos).

3. **Bloque constructivo**. Representa un componente de negocios (potencialmente reusable), un componente de tecnología de información o una capacidad arquitectural que combina otros bloques constructivos.

   Los bloques constructivos pueden ser definidos en varios niveles: ABBs (Architecture Building Blocks) típicamente describen la capacidad requerida en la forma o SBBs (Solution Building Blocks) que representan componentes que son usados para implementar una capacidad requerida.

RESULTADO ESPERADO

Hay dos niveles de certificación:

1. **Nivel 1**. Conocido como Fundación TOGAF 9.
2. **Nivel 2**. Conocido como Certificado TOGAF 9. El nivel 2 contiene los requisitos de aprendizaje para el Nivel 1.

El Programa está diseñado para seguir las mejores prácticas de la industria para los programas de certificación equivalentes.

El primer nivel de certificación valida que el candidato tenga el conocimiento de los conceptos y terminología básicos de TOGAF 9 y comprende los principios básicos de la arquitectura empresarial. El segundo nivel, valida que el candidato sea capaz de analizar y aplicar los conocimientos de TOGAF.

Se realizan cuatro exámenes:

1. **TOGAF 9 Parte 1.** Se debe obtener una puntuación de 22 sobre 40 puntos, las preguntas son de opción múltiple.
2. **TOGAF 9 Parte 2.** Se debe obtener una puntuación de 24 de 40 puntos, solo son 8 preguntas a libro abierto, las respuestas correctas valen 5 puntos, la segunda mejor respuesta vale 3 puntos y la tercera mejor respuesta vale un punto.
3. **TOGAF 9 Combinando parte 1 y parte 2**. Para los candidatos que deseen alcanzar el nivel 2 de certificación directamente en un único examen, la descripción de este corresponde con los exámenes descritos anteriormente (Ilustración 10).
4. **TOGAF 8 – 9 Avanzado**. La primera sección es de 20 preguntas de opción múltiple que cubren el nivel 1 (los resultados del aprendizaje). Para obtener un pase para esta sección se requieren de 12 o más puntos sobre un máximo de 20. La segunda sección es idéntica al examen TOGAF 9 Parte 2 y se requieren 24 o más puntos de un máximo de 40 para pasar.

Los exámenes de certificación tienen un precio alrededor de USD 400 cada examen.

Los principales apartados son:

- **Arquitectura**
    - Sistema Operativo y Hardware
    - Servicios de software y middleware.
    - Aplicaciones
    - Información de gestión.
        - Hosting, tipos de datos e intercambio.
        - Métodos de acceso.
    - Seguridad
    - Sistema de Gestión.
    - Arquitectura del sistema de ingeniería en general.
        - Procesadores.
        - Servidores
        - Clientes
    - Métodos de ingeniería de sistemas y herramientas.
- **Arquitectura de las Guías de Cumplimiento de Revisión**.
    - Directrices para la adaptación.
    - Directrices para realizar el cumplimiento de la arquitectura.
- **Roles**
    - Niveles de gobierno dentro de la empresa.
    - Administración de las TI. Es una clave de la capacidad, requisitos y recursos para la mayoría de las organizaciones.

# Rqmt.	Requerimiento Base y Comentario	Nivel	Referencia de donde deriva el requerimiento	Documento donde la evidencia es encontrada	Referencia en el documento	Comentario del aspirante	Comentario del asesor
6	El proveedor de ATTC debe der estable financieramente, demostrado por un reporte financiero, un balance aprobado por un auditor independiente. El requerimiento puede cumplirse mediante la presentación de las cuentas auditadas de los dos años anteriores, o un plan de negocio en caso de puesta en marcha.	Necesario	ACR 4 Requerimientos de la Organización				
7	El proveedor de ATTC deberá poner en práctica procedimientos eficaces para el registro e identificación de los candidatos. Tales procedimientos deben estar documentados y sujetos a la libre auditoría (véase la lista de comprobación 11)	Necesario	ACR 4.2 Procesos y Sistemas de Calidad				
8	Todos los aspectos de la administración del curso, la entrega y el mantenimiento deberán estar cubiertos por un sistema de la calidad del documento. Documentación del sistema de calidad no tiene por qué ser siempre en la instancia primera pero debe proporcionarse dentro de los seis meses de la acreditación inicial. El proveedor de ATTC debe definir cómo se asegura la conformidad de los ATTS a los requisitos de acreditación antes del establecimiento de un sistema de calidad documentado.	Necesario					

Ilustración 10. Plantilla de TOGAF.

1.2.13 IT BASELINE PROTECTION MANUAL

El manual de protección base de TI presenta un conjunto de recomendaciones de seguridad, establecidas por la Agencia Federal Alemana para la Seguridad en Tecnología de la Información (BSI, en alemán Bundesamt für Sicherheit in der Informations Technik).

Este estándar plantea en forma detallada aspectos de seguridad en ámbitos relacionados con:

- **Aspectos generales.** Relacionado con la actividades de la organización y sus procedimientos además manejo de la información y datos
    - Gestión humana. Manejo y administración del recurso humano de la organización.

- Criptografía. algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican

- Manejo de virus. Prevención y manejo apropiado de virus informáticos evitando problemas subsecuentes.

- **Infraestructura.** la infraestructura en la que se apoya los procedimientos y actividades de la organización

    - Edificaciones. Construcciones de uso especifico y su respectivas instalaciones

    - Redes Wifi. redes de comunicaciones inalámbricas propensas a hackeo he intrusión.

- **Sistemas.** Sistemas operacionales o de desarrollo que proveen el funcionamientos de aplicaciones y requerimientos para los procesos de una organización

    - Windows. Sistema operativo basado en ventanas.

    - Novell. Plataforma de servicio para ofrecer acceso a la red y los recursos de información, sobre todo en cuanto a servidores de archivos

    - Unix. Sistema operativo portable, multitarea y multiusuario

- **Redes.** Cableado, dispositivos y topologías de redes**.**

    - Firewalls. parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

    - Módems. dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica o del cable.

- **Aplicaciones.** Aplicaciones específicas o propietarias para la operación de la organización

    - Correo electrónico. servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos

    - Manejo de la web. Administración y manejo de web

    - Bases de datos. Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso

El manual de protección base de TI presenta un conjunto de medidas de seguridad estándar recomendadas para sistemas de TIC's. El blanco de estas recomendaciones del manual de protección base de TI es alcanzar un nivel de seguridad para sistemas de las TIC's que es razonable y adecuada para satisfacer requerimientos de protección que también pueden servir como la base para sistemas de las TIC's y aplicaciones que requieren un alto grado de protección. Esto es logrado mediante la aplicación de estándares de seguridad organizacional, personal, infraestructural y técnicas. Para facilitar la estructuración y procesamiento de áreas de las TIC's, incluyendo el entorno operacional, el manual de protección base de TI está estructurado de una manera modular. Los módulos individuales reflejan áreas en las cuales las TIC's son empleadas, por ejemplo:

- Redes cliente/servidor
- Edificios
- Comunicaciones
- Componentes de aplicaciones.

Cada módulo comienza con una descripción de amenazas que pueden ser esperadas en el área dada, junto con su probabilidad de ocurrencia. Este "escenario de amenaza" provee la base para generar paquetes de medidas específicas para las áreas de:

- Infraestructura
- Personal
- Organización
- Hardware
- Software
- Comunicaciones
- Planes de contingencia

Los escenarios de amenaza están presentados de modo que puedan crear alertas, y no se requiere nada más para la creación de un concepto de seguridad producido por manual de protección base de TI. Es suficiente con identificar los módulos que son relevantes para el sistema o activos de TI bajo consideración e implementar de manera consistente todas las buenas prácticas recomendadas en esos módulos.

Usando el manual de protección base de TI, es posible implementar conceptos simples y económicos en términos de los recursos requeridos. Bajo la aproximación tradicional de análisis de riesgos, antes que nada las amenazas deben ser identificadas y asignadas con una probabilidad de ocurrencia y los resultados de este análisis serán utilizados para seleccionar las medidas apropiadas para las TI, dado que el riesgo residual restante puede ser determinado.

Por otro lado, la aproximación adoptada en el manual de protección base de TI sólo requiere de una comparación entre el objetivo y la situación actual para llevar a cabo las medidas recomendadas y las ya implementadas.

Los defectos de seguridad necesitan ser eliminados a través de la adopción de las medidas de seguridad que faltan o no han sido implementadas.

Sólo donde el requerimiento de protección es alto es necesario también llevar a cabo un análisis de seguridad suplementario, tomando en cuenta el costo que implica implementar esas medidas adicionales. Sin embargo, por lo regular es suficiente implementar las recomendaciones hechas en manual de protección base de TI con medidas adaptadas y más rigurosas, que están descritas detalladamente en el manual que sirve como instrucciones específicas de implementación.

Con respecto a la técnica usada, se ha tenido cuidado en asegurar que las descripciones sean entendibles para aquellos que tienen que implementarlas ya sea por un administrador experimentado o un usuario. Teniendo en mente el paso de la innovación y cambios de versión en el área de las TIC's, el manual de protección base de TI ha sido diseñado para hacer fácil su utilización.

El BSI trabaja continuamente y actualiza los módulos existentes en intervalos regulares para mantener las recomendaciones hechas en el manual en línea con los últimos desarrollos tecnológicos.

RESULTADO ESPERADO

El manual de protección base de TI comprende medidas de seguridad básicas para sistemas típicos de TI con necesidades de protección normales.

La detección y evaluación de puntos débiles en los sistemas de TI con frecuencia ocurre en la Evaluación de Riesgos, donde una amenaza potencial es evaluada y los costos de daño al sistema son investigados individualmente. Este acercamiento consume mucho tiempo y también es muy caro.

La protección procede desde una típica amenaza potencial, que se aplica al 80% de los casos y recomienda las medidas adecuadas en contra, de esta forma un nivel de seguridad puede ser alcanzado y visto como adecuado en la mayoría de los casos y en consecuencia reemplazando la evaluación de riesgos que en esencia es más cara.

- **Aspectos generales.** El primer nivel concierne a cuestiones organizacionales afectando gestión, personal o subcontratación.

- **Infraestructura**. Se centra en aspectos estructurales. Tratada por Técnicos internos.

- **Sistemas TI**. Este apartado concierne a las características de los sistemas de TI. Entre estas están incluidas, además de clientes y servidores, los PBX o máquinas de faxes. Tratada por Administradores de Sistemas.

- **Redes.** Aspectos de redes son incluidos en esta capa tratada por Administradores de Redes.

- **Aplicaciones TI.** Este apartado abarca las cuestiones relevantes en software como:
    - Bases de datos
    - Sistemas de gestión
    - E-mail
    - Servidores web.

  La situación de la amenaza se deduce a través de una descripción del componente examinando los hechos.

  Las medidas necesarias son presentadas en texto con ilustraciones cortas. El texto sigue los hechos del ciclo de vida en cuestión e incluye planeación y diseño, adquisición, realización, operación, selección y medidas preventivas.

  Después de realizar una deducción, las medidas individuales son recolectadas en una lista, que es ordenada de acuerdo con la estructura del catálogo de medidas y no de acuerdo con el ciclo de vida (Ilustración 11).

  Las medidas son ordenadas en categorías A, B, C, y Z:

    - **Categoría A.** Medidas para el punto de entrada en el tema.
    - **Categoría B.** Medidas que expanden la categoría A.
    - **Categoría C.** Medidas necesarias para una certificación del manual de protección base de TI.
    - **Categoría Z.** Presenta medidas adicionales que han sido probadas en la práctica.

  Para mantener cada componente tan compacto como sea posible será necesario recolectar aspectos globales en un componente, mientras que la información más específica es recolectada en un segundo. Ambos componentes, tanto el de aspectos globales como el de información específica deben ser implementados satisfactoriamente para garantizar la seguridad del sistema.

  Las respectivas medidas de amenazas, que son introducidas en el componente, pueden ser relevantes para otro componente en parte diferente. De este modo una red de componentes individuales surge en los catálogos del manual de protección base de TI.[14]

[14] http://auditoria20101.wikispaces.com/file/view/ITBaselineProtectionManual.pdf

Tabla de Sistemas IT planeados y existentes						
No.	Descripción y Sistema	Ubicación	Tipo	En red con	Estatus	Usuario
1	PERSO; Sistema UNIX	Bldg. 1	Servidor	Token-ring 1 Red personal Sin servicios	Se está probando	Div. 1
2	PBX, PBX-Annex	Bldg. 2	Independiente	...	Operacional	Todos
3	ENTE; Sistema Windows NT	Bldg. 2	Servidor	Ethernet segmento 2, red de trabajo, Internet, FTP	Operacional	Div. 6
4	PC-6.3-1. DOS-PC	Bldg. 2	Cliente	Ethernet segmento 2, Servidor #3	Operacional	Ref. 6.3
5	PC-6.3-2, DOS-PC	Bldg. 2	Cliente	Ethernet segmento 2, Servidor #3	Planificado	Ref. 5.4
6	PC-5.4-1, DOS-OC	Bldg. 3	Independiente	...	Planificado	Ref. 5.4

Ilustración 11. Plantilla IT Baseline[15]

1.2.14 NIST 800-14 (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)

En español significa Instituto Nacional de Estándares y Tecnología. La serie 800 es una serie de documentos de interés general sobre Seguridad de la Información, su publicación inició en 1990 y es producto de la unión de industrias, gobiernos y organizaciones académicas interesadas en la seguridad.

La publicación NIST 800-14 proporciona las mejores prácticas y principios de seguridad que pueden orientar al equipo de Seguridad en el proyecto. Este documento se debe combinar con otras publicaciones NIST para contribuir a la estructura necesaria del proceso de seguridad.

[15] (http://www.ntua.gr/nmc/bsi/english/b/22.htm)

Debe utilizarse para obtener detalles adicionales sobre cualquiera de las mejores prácticas que a continuación se mencionan.

- **Política**. Se refiere a la creación de un programa de seguridad informática, establece sus objetivos y asigna responsabilidades. También se refiere a las normas de seguridad específicas para sistemas particulares.

    - Programa de política. Se refiere a la creación y definición de un programa de seguridad informática, al establecimiento de las estrategias de la organización, la asignación de responsabilidades y verificación del cumplimiento de los puntos anteriores y en caso contrario la aplicación de sanciones. Debe ser claro en cuanto a qué recursos, incluyendo instalaciones, hardware, software, información y personal debe abarcar.

    - Problema específico de la política. Debe tratar sobre los temas de actualidad que preocupan a la organización y estar actualizados.

    - Sistema específico de la política. Debe centrarse en las decisiones. Mediante un análisis técnico gestionar las decisiones. Variar de acuerdo con las necesidades. Explicar quién puede hacer una acción sobre los registros de datos.

    - Todas las políticas deben ser apoyadas por la administración y ser consistentes con las demás leyes, directivas y procedimientos presentes en la organización.

- **Programa de Gestión .**Permite crear una estructura de soporte para la creación y administración de contenidos

    - Central de programa de seguridad. Proporciona distintos tipos de beneficios: mayor eficiencia y economía de seguridad en toda la organización.

    - Sistema de programa a nivel. Trata de los recursos de computación dentro de un elemento operativo, una aplicación importante, o un grupo de sistemas similares (ya sea tecnológicamente o funcionalmente).

- **Gestión de Riesgos**. Adopta medidas para reducir el riesgo a un nivel aceptable y mantener ese nivel de riesgo. Se requiere el análisis de riesgo en relación con los beneficios potenciales, la consideración de alternativas, y, finalmente, la aplicación de la gestión de lo que determina a ser el mejor curso de acción.

    - Evaluación de riesgos. Proceso de análisis e interpretación de riesgos. Identifica la parte del sistema que debe ser analizada y el método analítico. Después hace la recopilación y análisis de datos. Por último interpreta los resultados.

    - Mitigación de riesgos. Selecciona e implementa los controles de seguridad para reducir el riesgo a un nivel aceptable de gestión.

- Análisis de incertidumbre. Un análisis de incertidumbre se debe realizar y documentar de manera que el resultado se pueda utilizar.

- **Ciclo de planificación**. La mayoría contiene cinco fases básicas: inicio, desarrollo o adquisición, implementación, operación y disposición.

  - Plan de seguridad. Su objetivo es asegurar que las actividades de seguridad se llevan a cabo durante cada una de las fases.

  - Fase de iniciación. Se debe definir el propósito del sistema.

  - Fase de desarrollo o adquisición. El sistema es diseñado, comprado, programado, desarrollado y construido.

  - Fase de implementación. El sistema es probado e instalado.

  - Fase de operación o mantenimiento. El sistema está en marcha.

  - Fase de eliminación del ciclo de vida. Se dispone de información, hardware y software.

- **Personal o Herramientas de usuario.** Aplicaciones extra que ayudan al usuario a administrar y gestionar los recursos del sistema

  - Organización de personal.

  - Administración de usuarios. Asegurar la administración efectiva de acceso a las computadoras de los usuarios y mantener la seguridad del sistema, incluida la gestión de cuentas de usuario, la auditoría y la modificación puntual o eliminación del acceso.

- **Preparación para Contingencias y Desastres**. Un plan que tenga estrategias, métodos y recomendaciones para cualquier imprevisto los cuales contienen:

  - Plan de negocios.

  - Identificar recursos.

  - Desarrollar escenarios.

  - Desarrollar estrategias.

  - Probar y modificar el Plan.

- **Seguridad para el Manejo de Incidentes**. Manejar el ciclo de vida de todos los Incidentes. El objetivo principal del manejo de incidentes es devolver el servicio de TI a los usuarios lo antes posible

  - Uso de capacidad para el manejo de incidentes de seguridad informática.

- **Sensibilización y Capacitación**. Para que la seguridad informática sea eficaz se debe contar con una adecuada planificación, implementación, mantenimiento y evaluación periódica.

- **Consideraciones de seguridad en soporte informático y de operaciones**. Referente a la administración del sistema y las tareas externas al sistema para apoyar su funcionamiento, por ejemplo la documentación.

- **Seguridad física y ambiental**. De esta manera se previenen interrupciones en los servicios informáticos, daño físico, divulgación no autorizada de información, pérdida de control sobre la integridad del sistema y robo.

- **Identificación y Autenticación**. Ayuda a evitar que personas no autorizadas entren en un sistema informático. El sistema es capaz de identificar y diferenciar entre los usuarios.

- **Control de acceso lógico**. Referente a los medios contenidos en el sistema que permiten o restringen el acceso de alguna forma, estableciendo qué usuarios deben tener acceso sólo a los recursos que necesitan para realizar sus funciones oficiales.

- **Auditoría**. Pueden proporcionar un medio para ayudar a lograr varios objetivos relacionados con la seguridad, incluyendo la responsabilidad individual, reconstrucción de los hechos, detección de intrusos y la identificación del problema.

- **Criptografía**. Ayuda a proporcionar muchos servicios de seguridad, como la firma electrónica y garantizar que los datos no se han modificado.

RESULTADO ESPERADO

En esta metodología en lugar de llamarla organización, ya sea del tipo: comercial, fabricante, universidad, federal, estatal o local, nacional o extranjero; se le conoce como laboratorio, si esta organización realiza cualquiera de los métodos de ensayo incluidos en el Programa de Acreditación de Laboratorios (LAP) de acuerdo con el Cifrado y Comprobación de Seguridad (CST) puede solicitar la acreditación al Programa Nacional Voluntario de Acreditación de Laboratorios (NVLAP).

La acreditación se concederá si se cumplen las condiciones definidas en el documento NIST Handbook 150-17 y NIST Handbook 150 Checklist. La acreditación no implica una garantía de funcionamiento de los laboratorios o de los datos de prueba del sistema, sino que es un resultado de la competencia del laboratorio y la habilidad para la realización de las pruebas.

El NVLAP sigue la norma ISO/IEC 17043 para los tipos de ensayos de aptitud utilizados en el LAP CST. Esto consiste en verificar que las herramientas de prueba o componentes de funcionamiento sean identificadas y usadas adecuadamente por el personal de la organización, así mismo que dichas herramientas sean las apropiadas. Se debe

demostrar que se comprenden e interpretan correctamente los datos y resultados de las pruebas obtenidas de las herramientas de pruebas al igual que el conocimiento teórico y la experiencia técnica para alcanzar la acreditación. El cuestionario que se plantea hace preguntas para cada método de prueba para el laboratorio que busca la acreditación, las preguntas son relativas a cuestiones como criptografía, conocimientos de seguridad y conocimiento de normas que regulan (ilustración 12).

Los resultados del ensayo de aptitud se presentan por un evaluador dentro de los primeros 30 días a partir de haber concluido el proceso de pruebas.

4.3.2 Aprobación de documentos

4.3.2.1

OK a) Todos los documentos distribuidos entre el personal del laboratorio como parte del sistema de gestión deberán ser revisados y aprobados para su uso por personal autorizado antes de su emisión.

Ok

OK b) Una lista maestra o un procedimiento de control de documentos equivalentes que identifica el estado de revisión ocurrido y distribución de documentos en el sistema de gestión de ello se establecerá y estar fácilmente disponibles para evitar el uso de documentos no válidos y / u obsoletos.

La lista maestra está disponible en página de inicio del QMS; incluye la política de calidad y los 12 procedimientos de calidad.

4.3.2.2 Los documentos adoptados deben asegurar que:

OK a) Ediciones autorizadas de los documentos apropiados están disponibles en todos los lugares donde se realizan las operaciones esenciales para el funcionamiento eficaz del laboratorio.

Disponibles electrónicamente

OK b) Los documentos son periódicamente revisados, en caso necesario, para dar adecuación y cumplimiento de los requisitos aplicables.

Ok

OK c) Los documentos obsoletos son removidos prontamente de todos los puntos de emisión o uso, de otra manera se asegura que no sean utilizados.

Ok

OK d) Los documentos obsoletos son retenidos con fines de conservación ya sea legal o del conocimiento y están debidamente identificados.

Ok

4.3.2.3 Los documentos del sistema de gestión generados por el laboratorio deben ser identificados. Dicha identificación debe incluir:

OK a) La fecha de emisión y/o revisión de la identificación

OK b) La numeración de páginas

Ilustración12. NIST Handbook 150 Checklist.

Los principios de seguridad que examina son los siguientes:

- **Seguridad Informática como apoyo a la misión de la Organización**. Está basada en la misión de la organización, la visión y la cultura para garantizar el éxito del programa de seguridad de la información.

- **Seguridad Informática como un elemento integral de la buena gestión**. Una administración efectiva incluye planeación, organización, liderazgo y control.

- **Seguridad Informática rentable**. El costo de la seguridad de la información debe ser considerado como parte del costo del negocio, que incluye el costo de las computadoras, redes y sistemas de telecomunicaciones. Los propietarios de los sistemas tienen responsabilidades de seguridad fuera de sus propias organizaciones por lo que se debe asegurar la confidencialidad, integridad y disponibilidad de los sistemas.

- **Responsabilidades explícitas de seguridad y rendición de cuentas**. Las políticas deben identificar claramente las responsabilidades de los usuarios, administradores y gerentes. Las políticas deben ser documentadas, leídas, comprendidas y aceptadas por todos los miembros de la organización.

- **Seguridad Informática requiere un enfoque amplio e integrado**. Las tecnologías de la información, los usuarios y administradores deben participar en el proceso para desarrollar un programa completo de seguridad de la información. La seguridad informática debe ser evaluada periódicamente debido a que las tecnologías de información y comunicación, los datos, los usuarios, los riesgos con el sistema y los requisitos de seguridad son cambiantes.

- **Seguridad Informática limitada por factores sociales**. Las medidas de seguridad deben ser seleccionadas e implementadas con el conocimiento de los derechos e intereses de los demás. La seguridad puede mejorar el acceso y el flujo de datos e información, proporcionando información más precisa y confiable y una mayor disponibilidad de los sistemas.

1.2.15 ISO 9000

La serie ISO 9000 es un conjunto de cinco normas relacionadas entre sí, son normas genéricas, no específicas y que permiten ser usadas en cualquier actividad ya sea industrial o de servicios.

La importancia de la aplicación de las normas ISO 9000 para el desarrollo e implementación de sistemas de aseguramiento de la calidad radica en que son normas prácticas. Por su sencillez han permitido su aplicación generalizada sobre todo en pequeñas y medianas empresas.

Las normas ISO Serie 9000 brindan el marco para documentar en forma efectiva los distintos elementos de un sistema de calidad y mantener la eficiencia del mismo dentro de la organización.

La estructura de acción de las normas de aseguramiento de la calidad ISO serie 9000 es producto de un proceso evolutivo que puede resumirse en los siguientes pasos:

1. El cliente inspecciona los bienes entregados por el productor evaluando la calidad del producto.

2. Cuando el mercado pasa a manos de los compradores, estos aumentan sus exigencias respecto a la calidad total, fecha de entrega, precio, etc.

3. Comienzan a implementarse técnicas de control en la recepción, a los proveedores que entregan adecuadamente se les da la categoría de Calidad Certificada.

4. Posteriormente las empresas compradoras se dieron cuenta de que:

    a) Algunos proveedores aprobaban y pasaban piezas defectuosas provocando inconvenientes importantes en la producción.

    b) No se evitaban costos de producción que posteriormente pagaba el cliente.

5. Aparece entonces el sistema de aseguramiento de calidad implementado por el proveedor que consiste en controlar todos los factores que inciden en los resultados de la actividad, es decir, asegurar la calidad de manera que esta sea una consecuencia del proceso y no del control.

6. El comprador comienza a mirar cómo se desarrolla la actividad del proveedor e inclusive a quien le provee los insumos. La razón de esta intromisión es que únicamente auditando el sistema de calidad se asegura la continuidad y la economía de los procesos. Es el comienzo de las auditorias privadas.

7. Esto es costoso para el cliente (que debe pagar las auditorías) y para el proveedor que debe atender muchas auditorías de cada uno de los clientes. Se piensa así en la certificación por terceros asegurando al cliente el sistema de calidad con auditorías periódicas.

8. A fin de facilitar el control del cliente sobre el proveedor y lograr que los sistemas de aseguramiento de calidad sean auditables es que se generan las normas de aseguramiento de calidad.

9. La verificación del sistema del proveedor contra un sistema normalizado de aseguramiento de calidad es realizada por organismos externos a las partes (proveedor-cliente) denominadas Registradoras. Este mecanismo unifica requerimientos y optimiza costos.

10. La necesidad de generar confiabilidad en las Registradoras produjo la aparición de los Organismos de Acreditación, generalmente instituciones estatales

La relación entre las distintas partes que intervienen en los sistemas de aseguramiento de la calidad se visualiza en estructuras de acción de la norma ISO serie 9000.

La serie de normas ISO (Ilustración 13) destinadas al aseguramiento de la calidad están armonizadas entre sí y son:

- **ISO 9000.** Cumple el papel de eje distribuidor del sistema. Expone el alcance real de la serie. Define la filosofía general de las normas, los distintos tipos, niveles y pautas para la aplicación de las distintas normas.

- **ISO 9001.** Se aplica cuando la empresa debe responsabilizarse por todas las etapas del ciclo, es decir: diseño, desarrollo y elaboración.

- **ISO 9002.** Se aplica cuando las características del bien o servicio son definidas por el cliente.

- **ISO 9003.** Cubre las obligaciones de aseguramiento de calidad en las áreas de control final y pruebas. Es de limitada aplicación por lo que existen planes para su eliminación.

  En los casos de exigencia contractual, las normas aplicables son las normas ISO 9001/2/3. La norma a aplicar depende del alcance de la actividad de la empresa, no de una elección a voluntad.

- **ISO 9004-1/ ISO 9004-2.** Establecen condiciones y pautas para guiar a las empresas en la implementación de su propio sistema de aseguramiento de calidad. Su desarrollo no es válido para certificación o registro.

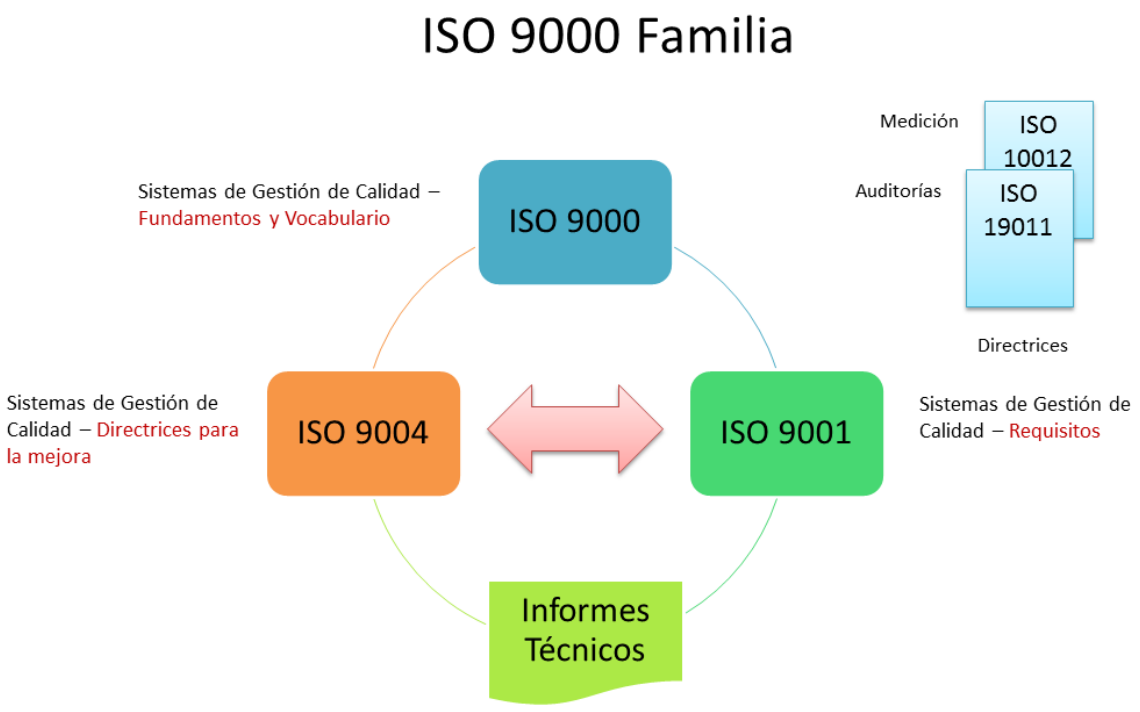


Ilustración 13. Familia ISO 9000

- **Calidad.** La totalidad de las características de una entidad que le confieren la aptitud para satisfacer las necesidades establecidas e implícitas.

- **Política de calidad.** Orientaciones y propósitos generales de un organismo concerniente a la calidad, expresados formalmente por el más alto nivel de la dirección.

- **Sistema de calidad**. La organización, los procedimientos, los procesos y los recursos necesarios para implementar la gestión de la calidad.

- **Aseguramiento de la calidad.** Conjunto de actividades preestablecidas y sistemáticas, aplicadas en el marco del sistema de la calidad, que han demostrado ser necesarias para dar la confianza de que una entidad satisfará los requisitos para la calidad.

- **Control de la calidad.** Técnicas y actividades de carácter operativo, utilizadas para satisfacer los requisitos de la calidad.

- **Proceso.** Conjunto de recursos y actividades relacionados entre sí que transforman elementos entrantes en elementos salientes.

- **Procedimiento.** Manera especificada de realizar una actividad.

RESULTADO ESPERADO

Se entiende por Certificación el documento emitido por un organismo acreditado que da fe de que el Sistema de Calidad de una organización cumple con los requisitos de la ISO 9001, ISO 9002.

La validez de la certificación es normalmente de tres años, debiendo realizarse auditorías de mantenimiento, que pueden ser anuales o semestrales, dependiendo de la compañía auditora. Transcurrido el período de tres años se efectúa una nueva auditoría de certificación completa.

Un proceso consiste en un grupo de actividades relacionadas y secuenciales que transforman las entradas, el material, la mano de obra, el capital, etc., en las salidas deseadas (bienes o servicios), añadiendo valor. Los procesos atraviesan las funciones de la organización, se orientan a resultados y muestran las relaciones proveedor/cliente entre funciones y cómo se realiza el trabajo realmente.

Tienen asociadas las siguientes características:

- Costo

- Plazo

- Impacto en calidad

- Valor añadido

Al ser procesos empresariales cabe citar el proceso de desarrollo de un nuevo bien o servicio, el proceso de tratamiento de reclamaciones, el proceso de créditos, el proceso logístico, el proceso del pedido, etc.

El proceso de implantación de la ISO 9000, constituye en sí mismo un proceso que debe iniciarse con un diagnóstico de la situación inicial de la empresa en relación con los requisitos del modelo ISO 9000.

1.2.16 MAAGTIC (MANUAL ADMINISTRATIVO DE APLICACIÓN GENERAL EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES)

Se trata de un manual para llevar a cabo los procesos en el área de Tecnologías de la Información de una Institución. Facilita una guía que describe las actividades, roles y productos de procesos críticos en Dirección, Control, Gestión y Operación de una unidad tecnológica; sumándole a esto una serie de indicadores que permitirán medir los resultados, efectividad y eficiencia de los procesos.

Este manual está basado en estándares como lo son: PMBOOK, CMMI, ITIL, ISO 27001, Balanced Score Card, TOGAF, ISO 9001, VAL IT, MOPROSOFT, RISK IT.[16] Se compone por 30 procesos estructurados por 11 grupos considerados en 4 niveles de gestión que describen que hay que abordar en cada uno de ellos (Ilustración 14):

- **Gobierno**
    - Dirección
        - Establecimiento del modelo de gobernabilidad de las TIC.
        - Planeación estratégica de las TIC.
        - Determinación de la dirección tecnológica.
    - Control
        - Administración de la evaluación de las TIC.
        - Administración de riesgos de las TIC.
- **Organización/Estrategia**
    - Administración de Proyectos

[16] http://elempresario.mx/matersys/que-es-maagtic

        - Administración del portafolio de proyectos de las TIC.
        - Administración de proyectos de las TIC.
    - Administración de Procesos
        - Operación del sistema de gestión y mejora de los procesos de la UTIC.
    - Administración de Recursos.
        - Administración del presupuesto de las TIC.
        - Administración de proveedores de productos y servicios de las TIC.
        - Administración de adquisiciones de las TIC.
    - Administración de servicios.
        - Administración del portafolio de servicios de las TIC.
        - Diseño de servicios de las TIC.

- **Ejecución/Entrega**
    - Administración y desarrollo de soluciones
        - Definición de requerimientos de soluciones.
        - Desarrollo de soluciones tecnológicas.
        - Calidad de soluciones tecnológicas.
    - Transición y entrega.
        - Administración de cambios.
        - Liberación y entrega.
        - Transición y habilitación de la operación.
        - Administración de la configuración.
    - Operación de servicios.
        - Operación de la mesa de servicios.
        - Administración de servicios de terceros.
        - Administración de niveles de servicio.

        - Administración de la seguridad de los sistemas informáticos.

- **Soporte**
    - Administración de Activos.
        - Administración de dominios tecnológicos.
        - Administración del conocimiento.
        - Integración y desarrollo personal.
    - Operaciones
        - Administración de la operación.
        - Administración de ambiente físico.
        - Mantenimiento de infraestructura.

Lo que se busca lograr es:

- Tener un manual de procedimientos que describa el marco rector de procesos de las TIC's.
- Demostrar que los registros o productos se están llevando a cabo de acuerdo al MAAGTIC.
- Mostrar la relación que se tiene con las demás unidades responsables, incluyendo planeación y operación.
- Crear una mesa de servicios como punto único de contacto para solicitar servicios y productos, así como para informar de incidencias y problemas.
- Los acuerdos de niveles de servicio con las unidades responsables, acompañados de una previsión presupuestal suficiente para proveer el servicio en los términos acordados.
- Contar con las herramientas para soportar el modelo de operación que exige el MAAGTIC.
- La recopilación de métricas e indicadores.

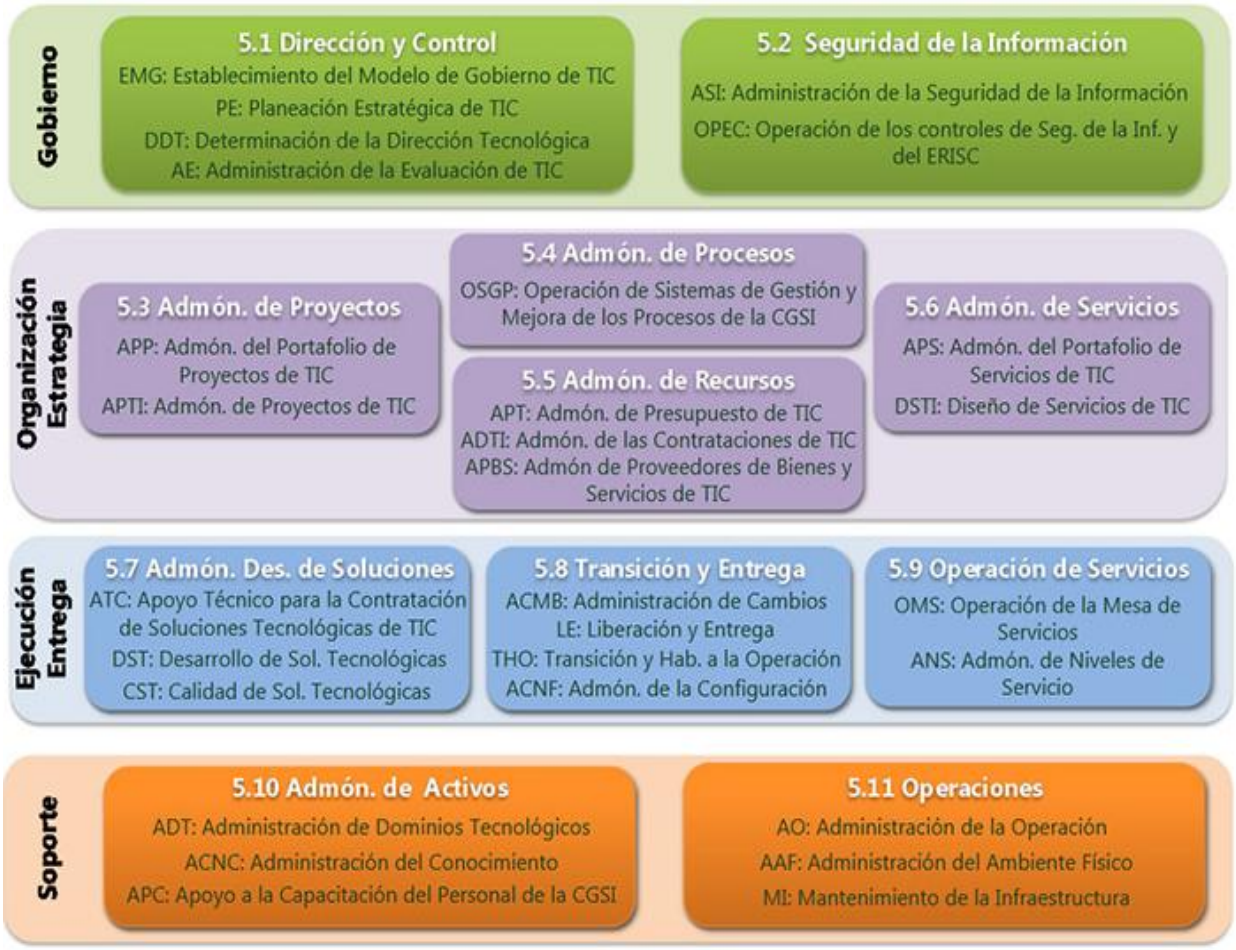


Ilustración 14. Niveles de Gestión de MAAGTIC. [17]

Se debe analizar la situación y tamaño actual de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC) tomando en cuenta recursos, infraestructura, servicios y capacidad de operación.

El manual requiere que se establezcan procesos de acuerdo con su marco rector, ello implica la documentación de los procesos y sus productos, así como establecer indicadores de evaluación y asignación de roles. Al detectar los elementos que conforman los procesos se entenderá el mecanismo de los mismos. Se debe formar un equipo de trabajo en el cual se incorpore personal de los niveles más altos de la institución, asignar roles y responsabilidades y comunicarlo a todos los integrantes. Se debe establecer una fecha límite para generar ajustes a los documentos y determinar un formato y estilo único.

Es necesario comunicar oportunamente y mantener informados a todos los empleados sobre los beneficios de adoptar los procesos y apegarse a ellos, para minimizar la resistencia y favorecer el éxito de la implantación.

[17] (http://www.cgsi.ipn.mx/MAAGTIC-SI/Paginas/Que-es.aspx)

Para abordar la implantación de MAAGTIC hay varias maneras:

- Iniciar por los procesos fáciles.
- Enfrentar los procesos complejos.
- Que la implantación de los procesos lo realice personal de mayor experiencia.
- Identificar las excepciones y darles un tratamiento especial.
- Buscar un punto medio en el grado de madurez de los procesos.

Por último concluir el documento de administración de procesos para poder iniciar la implantación. Lo que sigue es poner en marcha la implantación.

Es conveniente revisar que se lleven a cabo las actividades para poder confirmar o rectificar el camino. Por último viene una etapa de evaluación de resultados en la que se debe contar con evidencia documental de los procesos.

1.3 JUSTIFICACIÓN DE LAS METODOLOGÍAS SELECCIONADAS

Las metodologías elegidas para la realización de este apartado, han sido seleccionadas con base en los alcances y factores que se implementan universalmente para la aplicación de estándares y normas. Ahora bien, todo esto aunado a la importancia que las Tecnologías de la Información y Comunicación (TIC) han alcanzado, ha dejado de ser una herramienta de soporte para convertirse en una necesidad para cualquier dependencia.

COBIT nos proporcionará un marco de referencia que nos asegurará que los recursos de las TIC's son utilizados, gestionados y dirigidos de manera adecuada y responsable. Nos ayudará a tomar en cuenta los objetivos, riesgos y recursos con los que cuenta la entidad.

Así mismo nos ayudará a lograr una mayor adaptabilidad de los procesos de la entidad y ver la interrelación entre los objetivos de control de manera que se evite aislar los procesos para evitar distorsiones en el análisis y resultados de los mismos, por lo que COBIT proporciona el enlace entre COSO e ITIL.

Evaluar el cumplimiento de las normas internas de protección, así como los procedimientos y controles establecidos, recomendando y asesorando a la administración en la implementación de aquellos que se consideren convenientes para que las operaciones se realicen con seguridad y eficiencia, logrando el mejoramiento efectivo de la dependencia.

Para la gestión de seguridad, infraestructura, aplicaciones y el manejo de incidentes se utilizará ITIL.

De cualquier modo, son muchos los problemas que se presentan al gestionar estas TIC's, en el sentido de cómo lograr que éstas sean una ventaja para las dependencias y cómo hacer que las TIC's sean una inversión con retorno y no solamente un gasto innecesario.

Con todo esto y los posibles problemas que se pueden presentar en una organización, elegimos las metodologías que más se adaptan a las necesidades y se enfocan en brindar servicios de calidad para lograr la máxima seguridad. Para ello, se parte de un

enfoque basado en el triángulo procesos-personas-tecnología que determina la forma de ejecutar procesos estándar ayudados de la tecnología para lograr el cumplimiento satisfactorio del plan de seguridad y para el uso adecuado de los servicios de las TIC's por parte de los usuarios.

Por otro lado, quisimos establecer una guía que permita a las Organizaciones mejorar los procesos y su habilidad para organizar, desarrollar, adquirir y mantener productos y servicios informáticos respecto a sus procesos de seguridad, con el propósito de contrarrestar las vulnerabilidades adecuadamente y así cumplir con los objetivos del plan de seguridad.

Sabemos que los estándares no siempre encajan el uno con el otro ya que cada uno de ellos fue creado por personas diferentes, en un tiempo, un lugar y con un propósito diferente. Aunque pueden existir varios estándares que den solución a un determinado problema, cada uno de ellos fue creado para tratar un rubro específico, con un enfoque determinado y con un nivel de implementación distinto. Es necesario saber qué partes de cada estándar o modelo pueden ser utilizadas para cada caso.

En definitiva, es primordial saber elegir las mejores prácticas, manuales, guías, procesos y estrategias que abarcan todos estos modelos y así poder generar un modelo personalizado y adaptado totalmente para la realización de un diagnóstico que detecte problemas, vulnerabilidades o errores dentro de la organización.

Capítulo 2

CAPÍTULO II. PLAN DE SEGURIDAD DE UNA ORGANIZACIÓN

2.1DEFINICIÓN

Un plan de seguridad es un conjunto de requisitos, reglas y procedimientos mediante los cuales la organización previene, protege y maneja los recursos con los cuales cuenta. Es una descripción de lo que necesitamos proteger, de qué necesitamos protegerlo y cómo vamos a protegerlo.

El objetivo principal del plan de seguridad es concientizar a todo el personal de la necesidad de conocer qué principios rigen la seguridad de la organización y cuáles son las normas para conseguir los objetivos de seguridad.

Un plan de seguridad se compone de políticas que pueden ser:

- Prohibitivas. Si todo lo que no está expresamente permitido está denegado.
- Permisivas. Si todo lo que no está expresamente prohibido está permitido.

Cualquier política de seguridad debe contemplar los elementos clave en materia de seguridad de un sistema informático[18]:

- **Integridad**. Certificar que la información del sistema no ha sido modificada desde que fue almacenada por personal autorizado.
- **Disponibilidad**. Garantizar que los recursos del sistema estarán disponibles cuando se necesite acceder a ellos, cuando sea requerido y tantas veces como sea necesario por el personal autorizado.
- **Confidencialidad**. Se refiere a que la información sólo puede ser conocida por personal autorizado.
- **Control**. Considerar el control del acceso y registro del uso de los recursos protegidos e identificación de los usuarios.
- **Autenticidad**. Se refiere a que el sistema debe ser capaz de verificar la identidad de los usuarios a través de una contraseña, un número personal de identificación, alguna tarjeta para verificar su identidad, uso de algún biométrico, entre otros.
- **Utilidad**. Los recursos del sistema y la información que se maneja deben ser útiles para alguna función a desempeñar.
- **No repudio**. Hace referencia a que cuando se envía un mensaje el receptor pueda probar que este fue enviado por el emisor.

[18] Donn B. Parker. Demonstrating the elements of information security with threats. In *Processing of the 17th National Computer Security Conference*, pág. 421-430, 1994.

2.2CONTEXTO

2.2.1POLÍTICAS Y PROCEDIMIENTOS

Una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general del sistema.[19]

De acuerdo con la RFC 2196, la cual es una guía para el desarrollo de políticas y procedimientos de seguridad informática para los sitios que tienen sistemas en Internet, se define una política de seguridad como:

"…una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.[20]"

Cualquier política de seguridad debe contemplar los elementos clave en materia de seguridad: la Integridad, Disponibilidad, Privacidad, Control, Autenticidad, Utilidad y no repudio.

Un **procedimiento de seguridad** informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática[21]. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan, como son:

- **Preventivos**: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.

- **Detectivos**: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

- **Correctivos**: Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

- **Disuasivos:** Actúan manipulando las circunstancias para que el hecho no ocurra y así evitar las que sucedan.

[19] HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 1.2). Capítulo 16-Página 259.
[20] RFC 2196: Site Security Handbook. Fraser, Ed. Septiembre 1997. http://tools.ietf.org/html/rfc2196
[21] http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

2.2.2AMENAZAS Y VULNERABILIDADES

AMENAZAS

Una amenaza es todo aquello que puede, intenta o pretende destruir un activo. Es decir daños latentes que no se han concretado. Las amenazas se clasifican dependiendo de las fuentes que las generan, en:

a) **Naturales**. Surgen de las fuerzas naturales tales como inundaciones, los terremotos, el fuego, el viento. Dichos desastres hacen surgir amenazas directas, pues repercuten indiscriminadamente en el funcionamiento físico de las computadoras, redes, instalaciones y líneas de comunicación.

b) **Hardware**. Se dan por fallas físicas que presenta cualquiera de los dispositivos que conforman nuestro Site como desperfecto de los equipos, bajo rendimiento, deterioro o incorrecto funcionamiento, entre otros.

c) **Software**. Se presenta cuando un mecanismo de seguridad se implementa o se diseña en forma incorrecta incumpliendo con las especificaciones.

d) **Red**. Se presentan cuando no se calcula bien el flujo de información que va a circular por el canal de comunicación o por una desconexión del canal de comunicación o de varios equipos conectados a la red.

e) **Humano**. La amenaza surge por ignorancia, descuido, negligencia o inconformidad en el manejo de la información por parte del personal o simplemente por mala intención.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en dos partes:

- **La seguridad lógica**. Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

  Dicha seguridad tiene como objetivo restringir el acceso a los programas y archivos asegurando que se estén utilizando los datos y el procedimiento correctos, para que los operadores trabajen sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan, confiando en que la información recibida sea la misma que ha sido transmitida, verificando que existan sistemas alternativos secundarios o de emergencia para la transmisión entre diferentes puntos.

- **La seguridad física**. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; estos mecanismos son implementados para proteger el hardware y medios de almacenamiento de datos.

VULNERABILIDADES

Las vulnerabilidades son puntos débiles existentes en el activo o en el entorno que al ser explotados o aprovechados por una amenaza, ocasionan un ataque.

Las vulnerabilidades, dependiendo de las fuentes que las generan, se clasifican en:

a) **Naturales**. Se refiere al grado en que el sistema puede verse afectado por desastres ambientales o naturales.

b) **Hardware**. El no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento y el adquirir equipo de mala calidad, son algunos ejemplos de este tipo de vulnerabilidad.

c) **Software**. Ciertas fallas o debilidades de los programas del sistema hacen más fácil el acceso de personas no autorizadas y lo hacen menos confiable. Este tipo de vulnerabilidad incluye todos los errores de programación del sistema operativo u otras aplicaciones.

d) **Red**. La conexión de las computadoras a las redes supone un enorme incremento de la vulnerabilidad del sistema, aumentando considerablemente la escala del riesgo al que está sometido al aumentar la cantidad de usuarios que pueden tener acceso al mismo.

e) **Humano**. Algunos ejemplos son: contratar personal con el perfil psicológico y ético no adecuado, no tener personal para todas las áreas, el descuido, cansancio, maltrato al personal, mala comunicación con el personal.

f) **Infraestructura fisica**. La podemos encontrar en la estructura del edificio o entorno del sistema. La relacionamos con la posibilidad de poder entrar físicamente al lugar donde se encuentra el sistema para robar, modificar o destruir al mismo.

2.2.3 ESTÁNDARES

Existen algunos estándares de políticas de seguridad creados por países y por áreas (gobierno, medicina, militar, etc.), pero los internacionales son los definidos por la ISO (International Organization for Standardization).

Un estándar es una regla que especifica una acción o respuesta que se debe seguir a una situación dada, se trata de orientaciones obligatorias que buscan promover la implementación de políticas de alto nivel en la organización antes de crear nuevas políticas.

Para contemplar los elementos clave en materia de seguridad de un sistema informático, la ISO 27002 define los siguientes controles los cuales también hacen recomendaciones:

- **Seguridad organizacional**. Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, outsourcing, estructura del área de seguridad).

- **Clasificación y control de activos**. Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.

- **Seguridad del personal**. Formación en materia de seguridad, cláusulas de confidencialidad, reporte de incidentes, monitorización de personal.

- **Seguridad física y del entorno**. Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos, incluyendo los humanos, de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.

- **Gestión de comunicaciones y operaciones**. Este es uno de los puntos más interesantes desde un punto de vista estrictamente técnico, ya que engloba aspectos de la seguridad relativos a la operación de los sistemas y las telecomunicaciones, como los controles de red, la protección frente a malware, la gestión de copias de seguridad o el intercambio de software dentro de la organización.

- **Controles de acceso**. Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitorización de accesos.

- **Desarrollo y mantenimiento de sistemas**. Seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de software.

- Gestión de continuidad del negocio. Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes.

- **Requisitos legales**. Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica. En este apartado de las políticas se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal junto a todos los aspectos relacionados con registros de eventos en los recursos (logs) y su mantenimiento.

También se han propuesto otros modelos para representar las prácticas y competencias en materia de seguridad implantadas por una organización. Entre ellos, "Systems Security Engineering - Capability Maturity Model" (SSE-CMM) desarrollado por la Asociación Internacional de Ingeniería de Seguridad de Sistemas (ISSEA, www.issea.org) y en el que se distinguen cinco niveles de madurez:

- Nivel 1: Prácticas de seguridad realizadas de manera informal

- Nivel 2: Planificación y seguimiento de las prácticas de seguridad

- Nivel 3: Definición y coordinación de las políticas y procedimientos de seguridad

- Nivel 4: Seguridad controlada a través de distintos controles y objetivos de calidad

- Nivel 5: Implantación de un proceso de mejora continua

2.2.4 SERVICIOS DE SEGURIDAD

Mejoran la seguridad de un sistema de información y el flujo de la misma en una organización, se trata de servicios que están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad.

Es una actividad que mediante un dispositivo físico o lógico permite resguardar un activo, disminuir un daño o evitarlo. En términos generales y con base en su objetivo se agrupa en cuatro tipos de control:

- **Controles detectores**. Están orientados a detectar la presencia de amenazas o riesgos. Están asociados a los recursos, objetivos o metas. Descubren ataques y disparan controles preventivos y correctivos.

- **Controles preventivos**. Protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.

- **Controles correctivos.** Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

- **Controles disuasivos.** Son medidas encaminadas a desanimar a las personas, para que lleven a cabo acciones que podrían transformarse en amenazas para la operación. Por ejemplo, mensajes de no utilización de elementos inflamables dentro de las áreas de cómputo. Reducen la probabilidad de un ataque deliberado.

Los mecanismos de seguridad se encuentran relacionados con los servicios, ya que un mecanismo puede proteger uno o más servicios. Los mecanismos de seguridad necesarios para proteger un activo deben haberse analizado previamente para detectar cuáles son los más adecuados y qué servicios de seguridad deben proveer.

Es decir, la decisión de qué mecanismos se deben diseñar, desarrollar o implementar se lleva a cabo después de detectar los activos a proteger y de qué se deben proteger. Un mecanismo puede implementar uno o varios servicios de seguridad y el nivel de protección se basarán en la cantidad de servicios implementados o la robustez de éstos.

Como ejemplos de mecanismos de seguridad se tienen los datos que se enmascaran usando una clave especial y siguiendo una secuencia de pasos preestablecidos, conocida como “algoritmo de cifrado”. El proceso inverso se conoce como descifrado, usa la misma clave y devuelve los datos a su estado original fortaleciendo la confidencialidad.

Los servicios de seguridad se clasifican en 6 tipos:

1. **Control de acceso**. El acceso a un medio de información puede ser controlado ya sea a través de un dispositivo pasivo tal como una puerta cerrada, o a través de un dispositivo activo como puede ser un monitor.

2. **Confidencialidad**. La privacidad es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a algo. La forma más común de proteger las cosas en el mundo físico es el uso de candados y cerraduras.

3. **Integridad**. La integridad prevé que los datos no hayan sido modificados y que la secuencia original se mantenga durante la transmisión.

4. **Autenticación.** Con este mecanismo sólo se verifica la identidad a través de:

    - Algo que se sabe: una contraseña y un número personal de identificación.

    - Algo que se tiene: como una tarjeta o un pasaporte el cual es utilizado por el sistema para verificar la identidad.

    - Algo que se es: la voz y la retina que pueden identificar de quién se trata y pueden ser utilizados en el proceso de autenticación.

5. **No repudio**. Previene a los emisores o a los receptores de negar un mensaje transmitido, por lo que cuando el mensaje es enviado el receptor puede probar que el mensaje fue enviado por el presunto emisor.

6. **Disponibilidad**. Se cumple si las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario.

2.2.5 RESPONSABLES

Un responsable es una persona que tiene a su disposición recursos y deberes por desempeñar y quien ante algún incidente debe actuar obligatoriamente de la manera más apropiada para resolver los problemas que se presenten.

El responsable del área de sistemas se encarga de definir una serie de reglas para poder salvaguardar la seguridad del sistema de la organización, para definir estas reglas es más que recomendable basarse en normas, reglamentos, protocolos y estándares vigentes en el país. Las personas que participan en la elaboración de dichas políticas definidas anteriormente son:

- **Administrador**. Persona que gestionará los recursos a proteger.

- **Personas con autoridad**. Persona que podrá imponer la sanción (jefes de área, supervisores).

- **Responsable jurídico**. Persona que vigilará que se cumplan los derechos de los individuos.

- **Redactor**. Persona que se encargará de escribir las políticas con la redacción y ortografía debidas.

- **Usuario**. Persona que hará uso de los recursos proporcionados por el administrador.

Los responsables deben tomar en cuenta que una política incluye lo siguiente[22]:

1. La declaración de la política (cuál es la posición de la administración o qué es lo que se desea regular).

2. Nombre y cargo de quien autoriza o aprueba la política.

3. Nombre de la dependencia, del grupo o de la persona que es el autor o el proponente de la política.

4. Especificar quién debe acatar la política y quién es el responsable de garantizar su cumplimiento.

5. Indicadores para saber si se cumple la política.

6. Referencias a otras políticas y regulaciones en las cuales se soporta o con las que se tiene relación.

7. Enunciar el proceso para solicitar excepciones.

8. Describir los pasos para solicitar cambios o actualizaciones en la política.

9. Explicar qué acciones se seguirán en caso de contravenir la política.

10. Fecha a partir de la cual tiene vigencia la política.

11. Fecha de cuando se revisará la utilidad o la calidad de la política.

12. Incluir un medio de contacto junto con el nombre de las personas en caso de preguntas o sugerencias.

13. Utilizar lenguaje sencillo.

14. Escribirlo de tal modo que pueda leerlo cualquier miembro de la Organización.

15. Evitar técnicas o métodos particulares que definan una sola forma de hacer las cosas.

[22] Texto traducido y adaptado de "The Security Policy Life Cicle: Functions and Responsibilities" de Patrick D. Howard, Information Security Management Handbook, Editado por Tipton y Krause, CRC Press LLC, 2003. http://api.ning.com/files/u2gdYg06meFYaRrQcaCxfptLmTGcy2B8wrTgigBnj7JnOKqK3ya3pQkNHSxKqyYB-dFWd0WaYHhFvTBKv9bkG8b921Boq3f*/guia_para_elaborar_politicas_v1_0.pdf

2.2.6 MONITORIZACIÓN

El proceso de monitorización va de la mano del control del servicio, este ciclo es importante para proveer, dar soporte y mejorar los servicios. La monitorización consiste en la observación atenta de una determinada situación con el fin de detectar cambios a lo largo del tiempo, la monitorización implica:

- Monitorizar los elementos a configurar y actividades clave.
- Asegurarse de que se cumplen las condiciones establecidas y, en caso contrario, advertir al grupo adecuado.
- Asegurar que el rendimiento y utilización de los componentes, sistemas, etc. están dentro de un rango previsto.
- Detectar niveles anormales de actividad en la infraestructura.
- Detectar cambios no autorizados.
- Asegurar el cumplimiento de las políticas de la empresa.
- Rastrear las salidas al negocio y garantizar que casan con los requisitos de calidad y rendimiento acordados.
- Rastrear cualquier información empleada para medir los indicadores críticos de rendimiento.

Hay dos tipos de ciclos de monitorización:

1. Sistemas de ciclo abierto. Se refiere a la programación actividades específicas sin tener en cuenta las condiciones del entorno. Por ejemplo, un respaldo periódico, que se realiza sin importar las circunstancias del sistema.
2. Sistemas de ciclo cerrado. Se refiere a monitorizar un entorno con el fin de responder sólo a los cambios que se produzcan. Por ejemplo, obtener un balance de carga de una red, en el que se ejercen tareas de control sólo si la monitorización indica que se está sobrepasando el tráfico normal.

Así mismo, existen dos niveles de monitorización:

1. Monitorización y control internos. Cuando desde un equipo o departamento se controlan los elementos y actividades de esa misma unidad.
2. Monitorización y control externos. Cuando un equipo o departamento realiza el control de elementos y actividades que dependen de otros grupos, procesos o funciones.

Se pueden distinguir varios tipos de monitorización:

- Monitorización activa. Consiste en hacer una comprobación directa del estado de un sistema o dispositivo.
- Monitorización pasiva. Genera y transmite eventos a un agente de monitorización de forma automática.
- Monitorización reactiva. Está diseñada para ejecutar acciones al producirse cierto tipo de eventos o fallos.
- Monitorización proactiva. Se utiliza para detectar los patrones de eventos que predicen el fallo de un dispositivo.

- Medición continua. Enfoca la monitorización como un registro del rendimiento en tiempo real,
- Medición basada en excepciones. Se limita a notificar las interrupciones.

2.2.7 ACCIONES CORRECTIVAS Y PREVENTIVAS

Una acción correctiva ayuda a la organización a identificar y posteriormente a eliminar las causas que generan la no conformidad o incumplimiento de requerimientos del sistema de gestión de la calidad. Se hace para evitar que algo pueda a producirse.

Una acción preventiva es aquella acción tomada para eliminar la causa de una no conformidad o situación indeseable. Se toma para evitar que algo suceda.

Las acciones correctivas y preventivas en conjunto (apartados 8.5.2. y 8.5.3. de ISO 9001:2008) son unas herramientas básicas para la mejora continua de las organizaciones. El objetivo de estas acciones es eliminar las causas reales y potenciales de los problemas o las no conformidades, evitando así que estas incidencias puedan volver a repetirse.

Los factores que deben considerarse para realizar acciones correctivas y preventivas son los siguientes:

- **Apertura de la acción**. Se refiere a la iniciativa de implementar una acción correctiva y preventiva de acuerdo a los siguientes puntos:

    1. Reporte de Incidencia o Informe de no Conformidad. No todos los problemas que ocurren deben tener asociada una acción correctiva, se debe considerar la gravedad y frecuencia con que ocurre la incidencia.

    2. Resultados de auditoría. Los problemas encontrados a lo largo de los procesos de auditoría deben ser solucionados oportunamente con la acción correctiva. Los comentarios y observaciones de la auditoría son una importante fuente de acciones preventivas.

    3. Análisis de datos e indicadores. Los resultados de los indicadores deben analizarse periódicamente, al obtener un valor negativo o con tendencia negativa pueden generarse acciones correctivas y preventivas.

    4. Revisión del sistema por la dirección. Al menos una vez al año se debe revisar el correcto desempeño del sistema, así como su capacidad para obtener los resultados esperados; con base a estos resultados se pueden detectar necesidades que podrían orientarse a acciones correctivas y preventivas.

- **Análisis de causas**. Conocer la causa facilita la elección de la acción adecuada. El uso de diagramas causa-efecto (Ilustración 15 y 16) es una herramienta útil, también conocida como diagrama de Ishikawa o Esqueleto de Pescado, consiste en una representación gráfica de todas las posibles causas de un fenómeno.[23]

[23] GALGANO, Alberto. "Los siete instrumentos de la Calidad Total". Ediciones Díaz de Santos, S.A., Madrid: 1995, pág. 99.

Está compuesto por un recuadro (cabeza), una línea principal (columna vertebral) y 4 ó más líneas que apuntan a la línea principal formando un ángulo de 45° (espinas principales), mismas que poseen a su vez dos o tres líneas inclinadas (espinas), y así sucesivamente (espinas menores), según sea necesario. Al hablar de espinas nos referimos a las causas del problema a analizar.

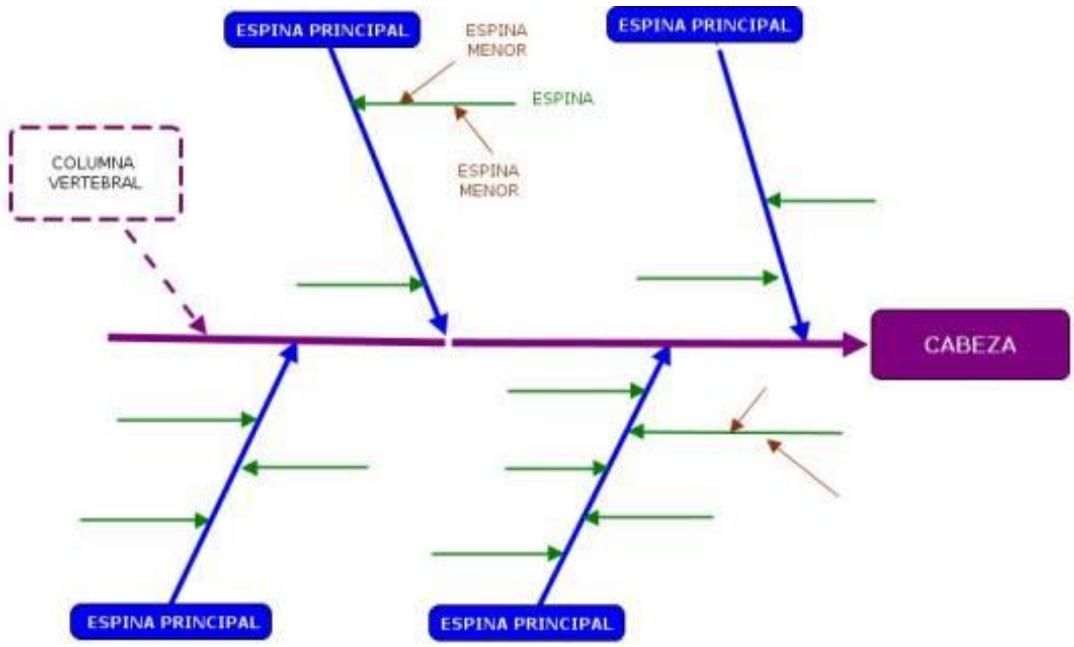


Ilustración 15. Estructura del Diagrama Causa-Efecto.

Un ejemplo aplicando este diagrama sería que el foco no enciende.

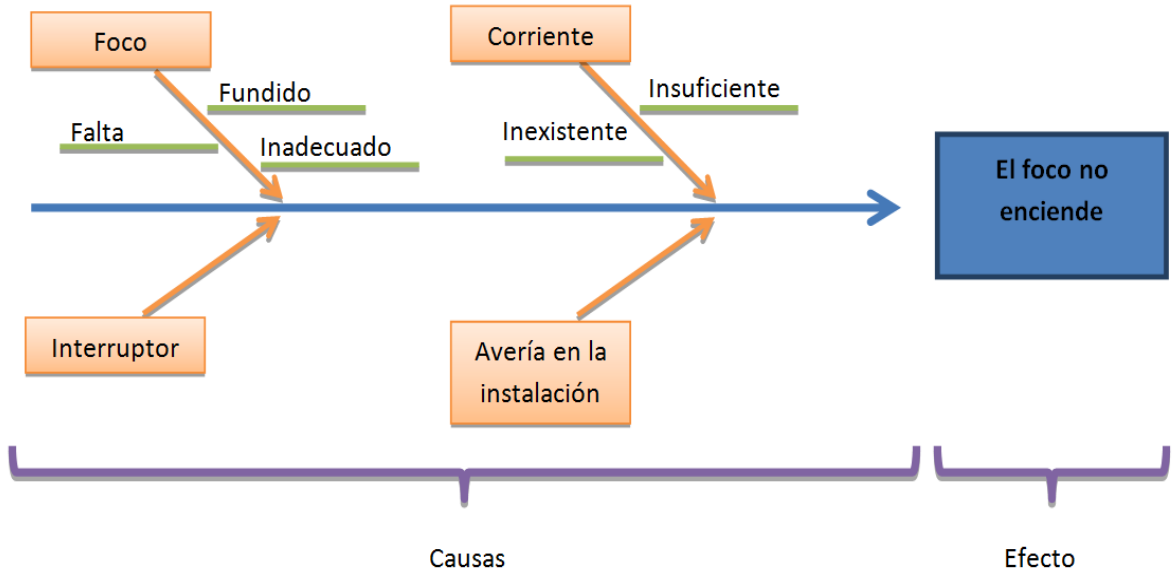


Ilustración 16. Ejemplo de aplicación del Diagrama Causa-Efecto

- **Planificación de actividades**. Las acciones para eliminar la causa de la no conformidad deben estar planificadas, esto significa que deben estar organizadas en el tiempo y que se deben definir los recursos y responsabilidades adecuados.

- **Resultados de acciones**. La organización debe registrar y verificar que se han llevado a cabo las acciones planificadas.

- **Verificación de eficacia**. Una vez realizadas las acciones se debe comprobar que han sido eficaces y que se ha eliminado la causa de origen de las no conformidades.

Al implementar las acciones correctivas y preventivas, se obtienen beneficios como la mejora contínua y la organización apta para implementar más medidas preventivas para hacer frente a los problemas que surgen en sus actividades.

Una metodología para el tratamiento adecuado de la Acción Correctiva consta de los siguientes pasos:

- **Detección de una No conformidad**. Considerar las posibles fuentes que pueden producir una no conformidad.

- **Aminorar el Efecto**. Resolver los desperfectos que la no conformidad ha causado mediante acciones inmediatas.

- **Análisis de los Síntomas**. Considerar que un síntoma "es la evidencia externa y medible de un problema".

- **Análisis de Causalidad**. Llegar a la identificación de la raíz de las causas ya conocidas, producto del análisis de los síntomas.

- **Definir la Acción Correctiva**. Evitar la repetición del problema.

- **Implantación de la Acción Correctiva**. Aplicar la acción correctiva correspondiente.

2.3 NIVEL DE IMPLEMENTACIÓN

Durante nuestra investigación hicimos una comparación de las metodologías y elegimos las que a nuestro juicio son las 5 áreas más importantes dentro del Site a revisar:

1. Energía

2. Control de acceso

3. Software

4. Hardware

5. Telecomunicaciones

El siguiente paso fue revisar el alcance de cada una de ellas y posteriormente generamos un cuestionario que en un principio constaba de 92 preguntas de opción múltiple en donde las opciones de respuesta las limitamos a 3 opciones (sí, no y no sé) pensando en las posibles repuestas que proporcionaría el responsable del área.

En un principio, hicimos el cuestionario usando la herramienta de Google Docs y debido a que rebasamos la cantidad de preguntas soportadas en memoria optamos por buscar otra herramienta que se llama Moodle, la cual está enfocada para hacer evaluaciones y nos permite administrar roles, como el de alumno, que en este caso se refiere a las empresas, también nos permite visualizar los resultados con varios niveles de detalle y exportarlos a Excel para poder hacer un análisis más profundo.

Inicialmente aplicamos el cuestionario a dos organizaciones en donde los respectivos responsables nos hicieron sugerencias y observaciones con las cuales elaboramos una segunda versión del cuestionario aumentando a 100 el número de preguntas.

Posteriormente, al aplicar el cuestionario con una tercera Organización el entrevistado también nos hizo comentarios y sugerencias que derivó en una tercera versión del cuestionario e inclusive optamos por agregar una nueva área denominada Administración.

Por otro lado nos dimos cuenta que hay preguntas que tienen una o dos preguntas derivadas por lo cual elegimos un criterio de evaluación de acuerdo con número de niveles o dependencias que se tuvieran.

a) Para una pregunta con dos derivaciones se optó por una ponderación de 0.6 y 0.4 para el caso de responder afirmativamente en los dos niveles (Ilustración 17). Partiendo del criterio que la primera pregunta depende de la segunda pregunta, si la primera pregunta es contestada ésta tendría un valor mayor, ya que la segunda pregunta dependería de la respuesta de la primera y por ningún motivo podría tener más valor la segunda respuesta si la respuesta de la primera es negativa, si las 2 son positivas se complementan obteniendo un valor de 1.

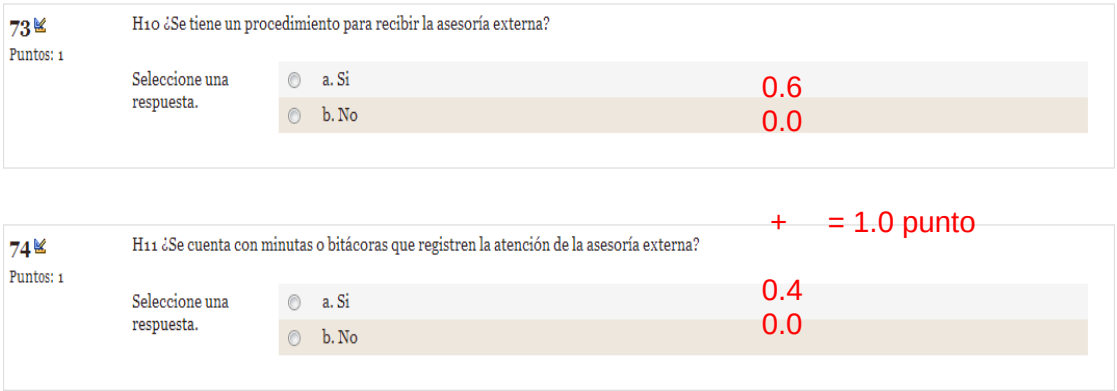


Ilustración 17. Pregunta con dos niveles

b) Para una pregunta que tenga tres derivaciones el criterio es 0.6, 0.2 y 0.2 para las respuestas afirmativas (Ilustración 18). Partiendo del criterio que la primera pregunta depende de la segunda pregunta y a su vez la tercera pregunta de la segunda pregunta, dependiendo de las respuestas, si la primera pregunta es

contestada afirmativamente ésta tendría un valor mayor, ya que la segunda dependería de la respuesta de la primera y la tercera dependería de la respuesta de la segunda y por ningún motivo podría tener más valor la segunda respuesta si la primera es negativa o la tercera si la segunda es negativa.

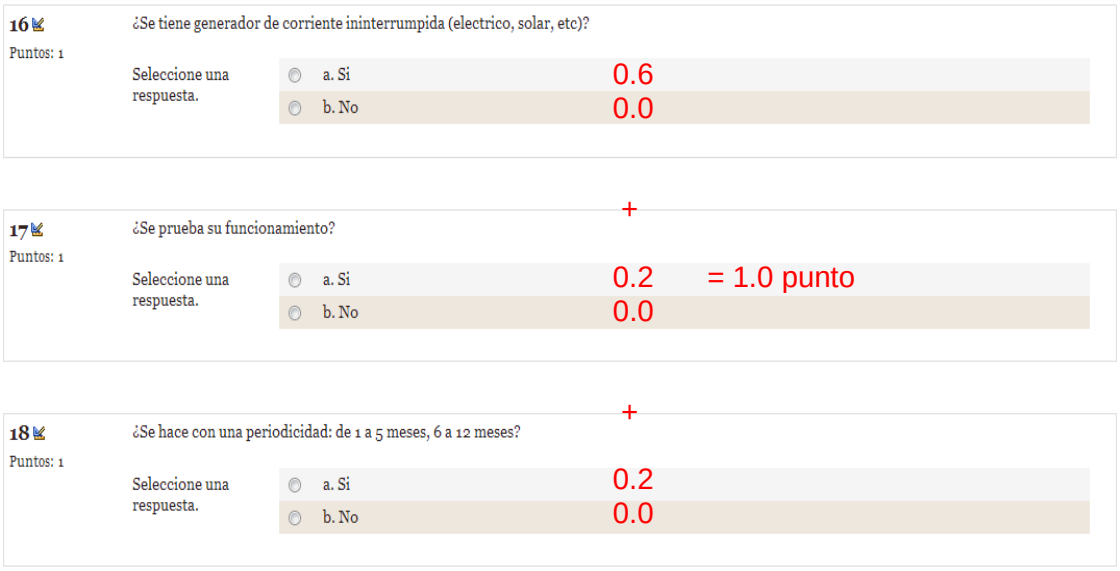


Ilustración 18. Pregunta con tres niveles

De esta forma al responder todos los niveles afirmativamente se obtiene el punto que designamos como valor máximo de la pregunta. Este criterio de ponderar con un mayor valor la primera pregunta lo elegimos debido a que la primera respuesta es la que tiene mayor peso sobre las otras.

Debido a la confidencialidad que nos pidieron guardar las organizaciones entrevistadas nos referiremos a ellas como O1, O2, O3, O4, O5, O6 y O7.

Para los subtemas siguientes nos limitamos a mencionar las organizaciones que obtuvieron una evaluación no satisfactoria.

2.3.3 POLÍTICAS Y PROCEDIMIENTOS

De acuerdo con lo investigado teóricamente, en el tema 2.2.1, se pudo constatar, las 7 organizaciones diagnosticadas no contaban con la documentación suficiente que acreditara las políticas y procedimientos.

Entre los procedimientos con los que no se cuenta está el de recepción de información, que es vital, porque si esta información llegara a caer en manos de terceros podría ser manipulada, dándole un mal uso que rompería con la integridad en el flujo de la información.

Respecto a las políticas de seguridad, se encontró que el reglamento de seguridad era inexistente, únicamente se contaba con un manual de uso del equipo de cómputo, lo cual no constituye un plan de seguridad. El manejo de la seguridad física se mantenía en regla

según las características del reglamento de COBIT, sin embargo la seguridad en el acceso no era conveniente.

Referente a la seguridad en la red LAN se contaba con un firewall configurado para filtrar el contenido malicioso que pudiera presentarse al navegar en internet, redes sociales y páginas con contenido para adultos.

El resguardo físico del equipo no era el adecuado debido a que cualquier persona podría acceder al CPD y provocar alguna avería debido a que los cables de conexiones en el área se encontraban expuestos a cualquier tirón o destrucción aunque en los demás lugares el cableado se encontraba debidamente protegido.

2.3.4 VULNERABILIDADES

De acuerdo con lo investigado teóricamente, en el tema 2.2.2, las vulnerabilidades encontradas en las 7 organizaciones se enfocaron en que la colocación de los equipos no era adecuada lo que incrementaba los riesgos de integridad por derrames de líquidos o fallas provocadas por el usuario. También, se encontraron incidentes que llevaron a la pérdida total de reguladores de energía.

En cuanto al software utilizado se descubrió que la gran mayoría era software ilegal, lo cual hace vulnerable a la organización en la realización de actividades que requieren software especializado, en muchas ocasiones el software era inadecuado y los parches en muchas otras ocasiones contenían software malicioso que puede causar estragos en sus sistemas.

Las vulnerabilidades en las redes eran más grandes, debido a que la red no estaba debidamente protegida contra intrusos, además de depender de una estación eléctrica la cual no tenía respaldo y en caso de presentarse algún incidente todo el personal se encontraría inactivo.

Las cuestiones ilógicas que también se presentaban con los usuarios eran entre otras el tener a la vista su clave de usuario y contraseña de acceso, lo que permitía que cualquier persona hiciera uso de ellos.

2.3.5 ESTÁNDARES

De acuerdo con lo investigado teóricamente, en el tema 2.2.3, para la O2 se encontró que si bien tienen las reglas a seguir en una situación dada, realmente no son implementadas aunque se cuente con ellas.

Para la O3 su instalación eléctrica está de acuerdo a la norma oficial NOM-001. Para O1, O2 y O3 se cuenta con los inventarios de sus activos, cláusulas de seguridad, reporte de incidentes y monitorización de personal, así como con la protección de malware, respaldo de la información, contraseñas y monitorización de los accesos.

Lo que falta implementar en algunas de las organizaciones es un plan de contingencias (O1, O2).

2.3.6 RESPONSABLES

De acuerdo con lo investigado teóricamente, en el tema 2.2.5, la O1 cuenta con un servicio de outsourcing para administrar el CPD y los responsables se encuentran implementando una serie de acciones para poder salvaguardar la seguridad de los sistemas.

La O2 cuenta con un reglamento de informática y cuenta con la firma de los usuarios que sustenta que lo han leído y saben que existe. Sin embargo no se verifica su cumplimiento.

2.3.7 SERVICIOS DE SEGURIDAD

De acuerdo con lo investigado teóricamente, en el tema 2.2.4, el acceso a la información se encuentra controlado con las cuentas de usuario definidas y los respectivos privilegios de acceso. El acceso a las instalaciones se hace, en su mayoría, mediante un dispositivo biométrico.

Sin embargo, respecto al ingreso al CPD en dos de las organizaciones (O1, O2) es completamente libre dado que cualquier persona puede estar en contacto con los servidores, pudiendo provocar algún desperfecto sin que la organización se entere debido a que no se cuenta con alguna cámara de vigilancia. Además de que sus CPD no están acondicionados y carecen de una instalación eléctrica únicamente para el equipo de cómputo.

2.3.8 MONITORIZACIÓN

De acuerdo con lo investigado teóricamente, en el tema 2.2.6, en general se cuenta con mecanismos de seguridad a los cuales se les aplica un algoritmo de cifrado.

También, cuentan con un sistema de detección de intrusos que monitorea la red de amenazas del exterior, y de esta forma se detectan los problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red.

Algunas organizaciones (O4, O5 y O6) cuentan con un firewall de hardware y software de manera que tienen una mayor protección.

Así mismo, todas las organizaciones cuentan con un antivirus para tener un control preventivo, detectivo y correctivo en caso de un ataque de virus al sistema.

2.3.9 ACCIONES CORRECTIVAS

De acuerdo con lo investigado teóricamente, en el tema 2.2.7, en todas las organizaciones cuentan con un Reporte de incidencias y de esta manera es fácil obtener la frecuencia y gravedad con la que se presentan los incidentes y tener una acción correctiva.

Para la O1 apenas se está implementando el uso de esta herramienta. No obstante, no se tiene un análisis de datos e indicadores de avance en la solución de los incidentes. Por otro lado, no se cuenta con un plan de trabajo que establezca cuales son las actividades y el tiempo en que se deben llevar a cabo, así como los recursos necesarios.

2.4 DIAGNÓSTICO

Una vez concluido el proceso de investigación, la selección de las áreas de interés y el diseño del cuestionario a aplicar, nos enfocamos en la búsqueda de organizaciones en las cuales pudiésemos aplicarlo.

Quisimos en primer instancia seleccionar organizaciones de diferentes tipos para poder contrastar los resultados es así que las siete organizaciones consultadas pertenecen al sector de servicios informática, publicidad, servicios escolares, administración escolar, administración pública y tienda departamental.

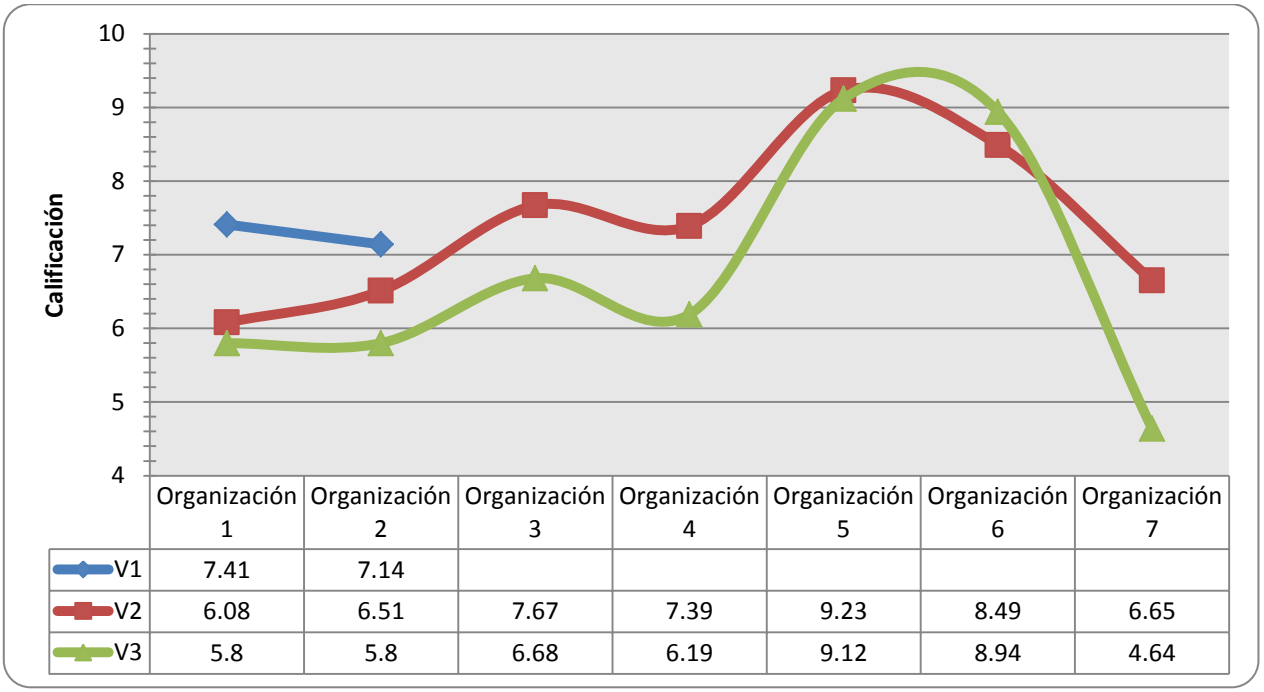
El proceso de aplicación del cuestionario duró cerca de dos meses debido a que tuvimos que generar nuevas versiones de acuerdo con la siguiente tabla 1.

Tabla 1. Versiones del cuestionario.

Versión	Número de preguntas	Número de Organizaciones
V1	92	2
V2	100	7
V3	112	7

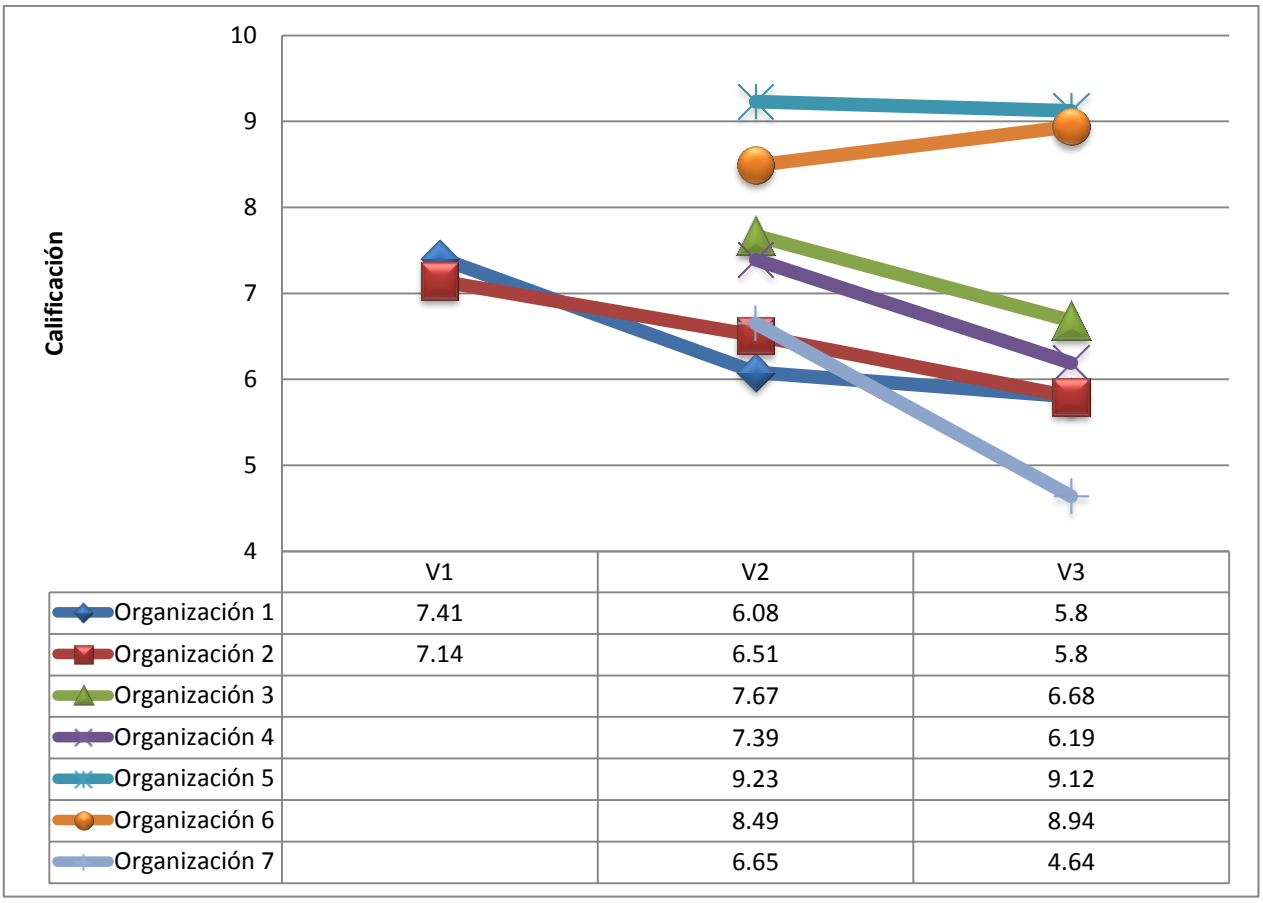
2.4.3 ANÁLISIS DE RESULTADOS

A continuación se presentan las calificaciones de las organizaciones respecto a las diferentes versiones del cuestionario (grafica 1 y 2).



	Organización 1	Organización 2	Organización 3	Organización 4	Organización 5	Organización 6	Organización 7
V1	7.41	7.14					
V2	6.08	6.51	7.67	7.39	9.23	8.49	6.65
V3	5.8	5.8	6.68	6.19	9.12	8.94	4.64

Gráfica 1. Calificaciones según la versión



	V1	V2	V3
Organización 1	7.41	6.08	5.8
Organización 2	7.14	6.51	5.8
Organización 3		7.67	6.68
Organización 4		7.39	6.19
Organización 5		9.23	9.12
Organización 6		8.49	8.94
Organización 7		6.65	4.64

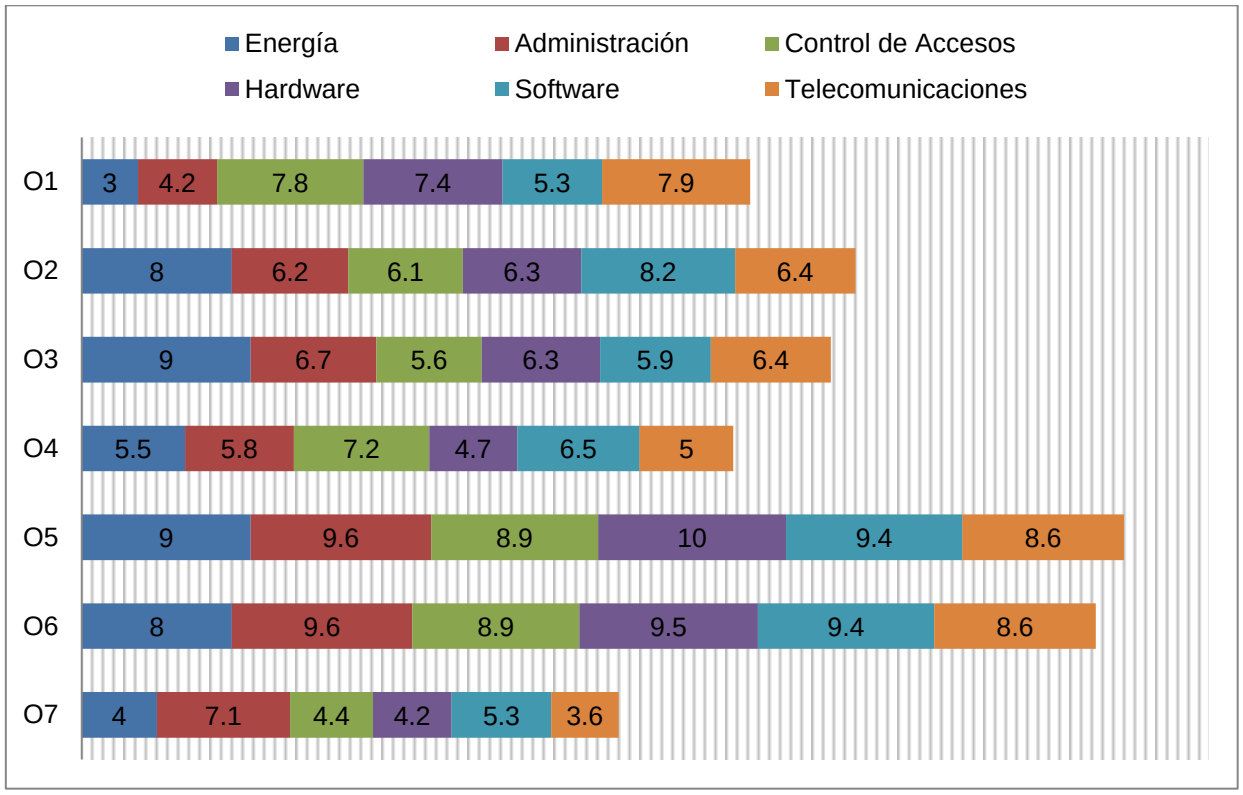
Gráfica 2. Calificaciones según la organización.

Como se puede observar en la gráfica 1 las calificaciones de las organizaciones a través de las tres versiones del cuestionario cambió bastante. Algunas organizaciones como O1 y O2 obtuvieron una calificación no aprobatoria al hacer modificaciones en los criterios de evaluación e incrementar el número de preguntas.

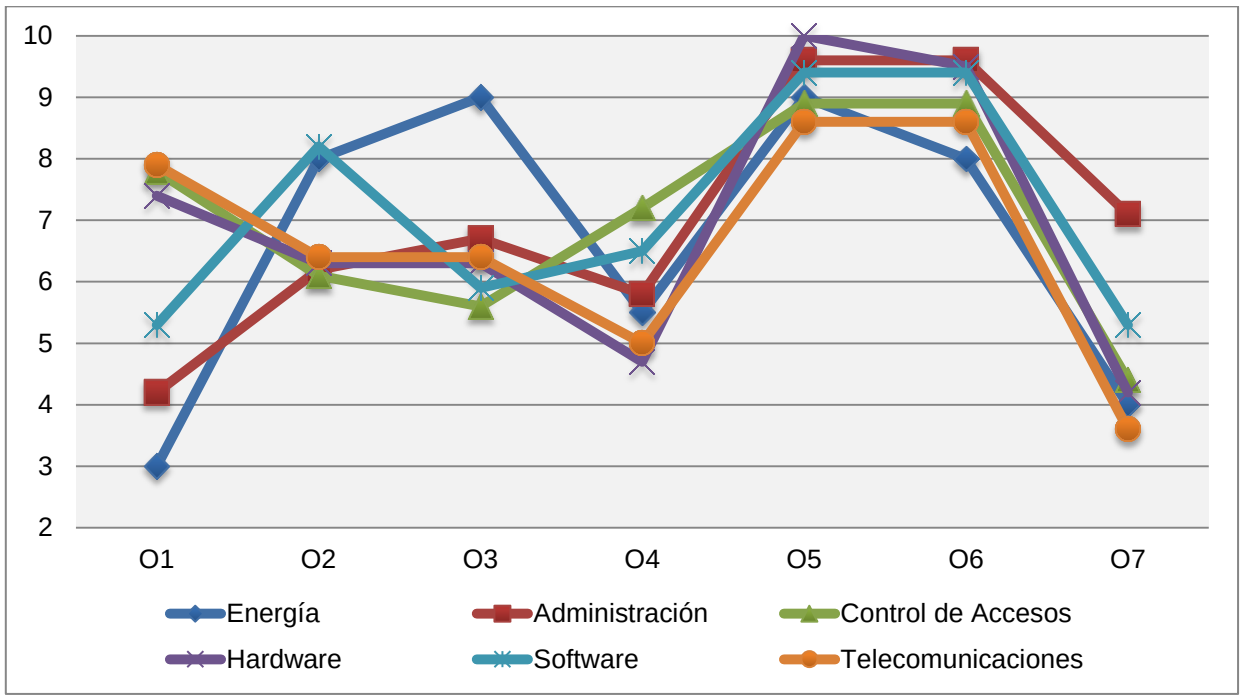
De la versión 2 a la versión 3 la calificación de la mayoría de las organizaciones bajaron su calificación, a excepción de la organización 6 que incrementó en décimas su calificación, de 8.49 a 8.94, esto debido a que el incremento de preguntas implicó un mayor detalle en las áreas a evaluar y esto ayudó a la organización a cubrir deficiencias que tenía en algunas de las otras áreas.

La gráfica 3 y gráfica 4 expresan lo mismo pero de distinta manera.

- O1, O5 y O6 tienen el más alto porcentaje para el área de telecomunicaciones.
- Para el área de software la más alta fue O2, O5 y O6.
- En el área de hardware las más altas fueron O1, O5 y O6.
- Para el área de energía O2, O3, O5 y O6 son las de mayor porcentaje obtenido.
- En el control de accesos O1, O3, O5 y O6 son las más altas.
- Para el área de Administración las más altas fueron O5,O6 y O7.
- Las organizaciones que se mantuvieron constantes son O5 y O6.



Gráfica 3. Porcentaje por Área de acuerdo con la Organización



Gráfica 4. Calificación por Área de acuerdo con la Organización

Gráficas de acreditación por área de acuerdo con la organización

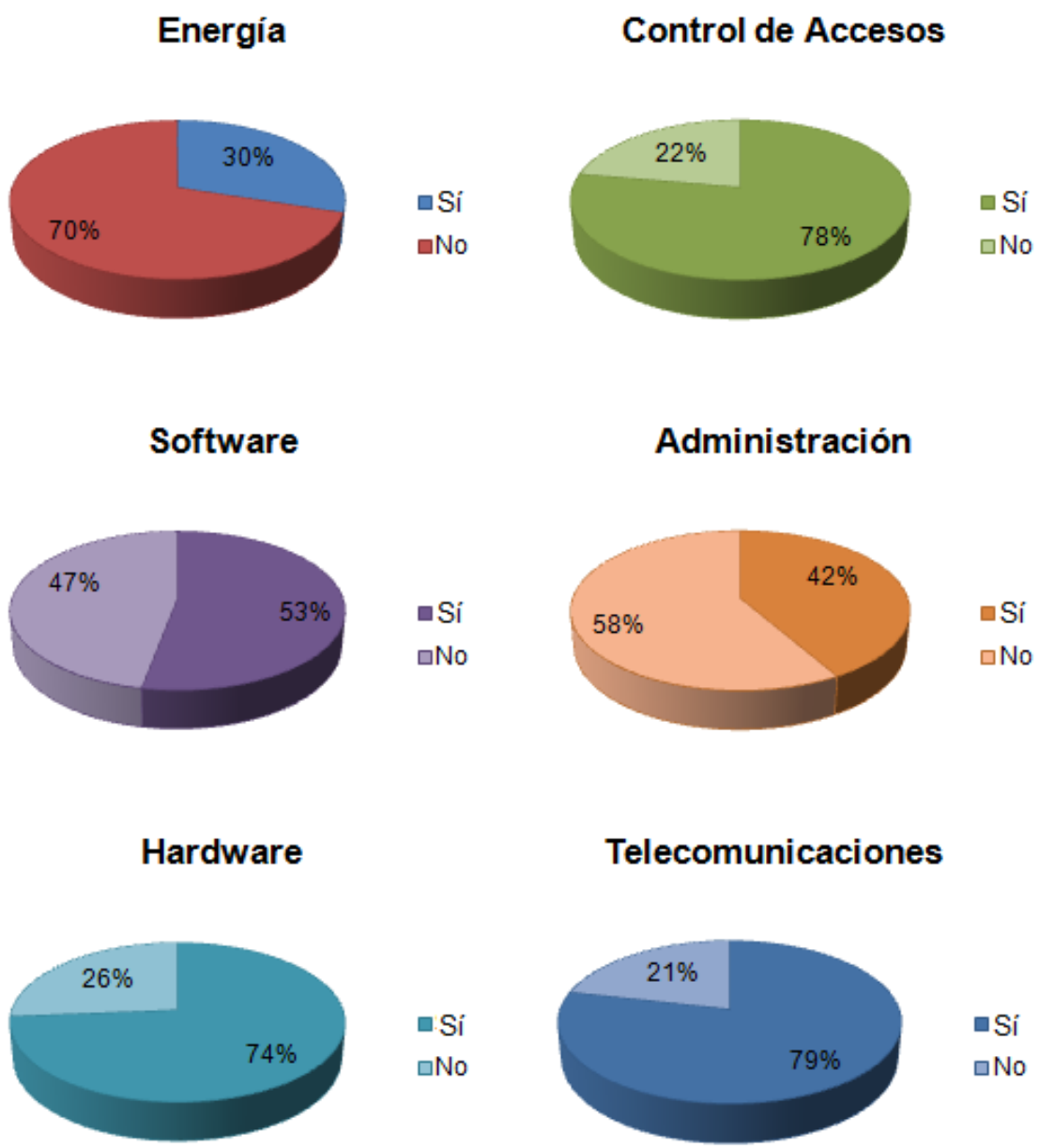
Para el análisis de resultados decidimos por establecer un criterio de valoración, para ello obtuvimos la media aritmética de las calificaciones de todas las áreas y para todas las organizaciones, lo cual nos dio un valor redondeado de 7 (tabla 2).

Es así que, calificaciones por debajo de 7 las consideramos no satisfactorias y por arriba de 7 las consideramos satisfactorias.

Tabla 2. Concentrado de valores que obtuvo cada organización

Organización	O1		O2		O3		O4		O5		O6		O7		Total
	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	
Energía	6	14	16	4	18	2	11	9	18	2	16	4	8	12	20
Administración	10	14	15	9	16	8	14	10	23	1	23	1	17	7	24
Control de Accesos	14	4	7	11	10	8	13	5	16	2	16	2	8	10	18
Hardware	14	5	12	7	12	7	9	10	19	0	18	1	8	11	19
Software	9	8	14	3	10	7	11	6	16	1	16	1	9	8	17
Telecomunicaciones	11	3	5	9	9	5	7	7	12	2	12	2	5	9	14
															112

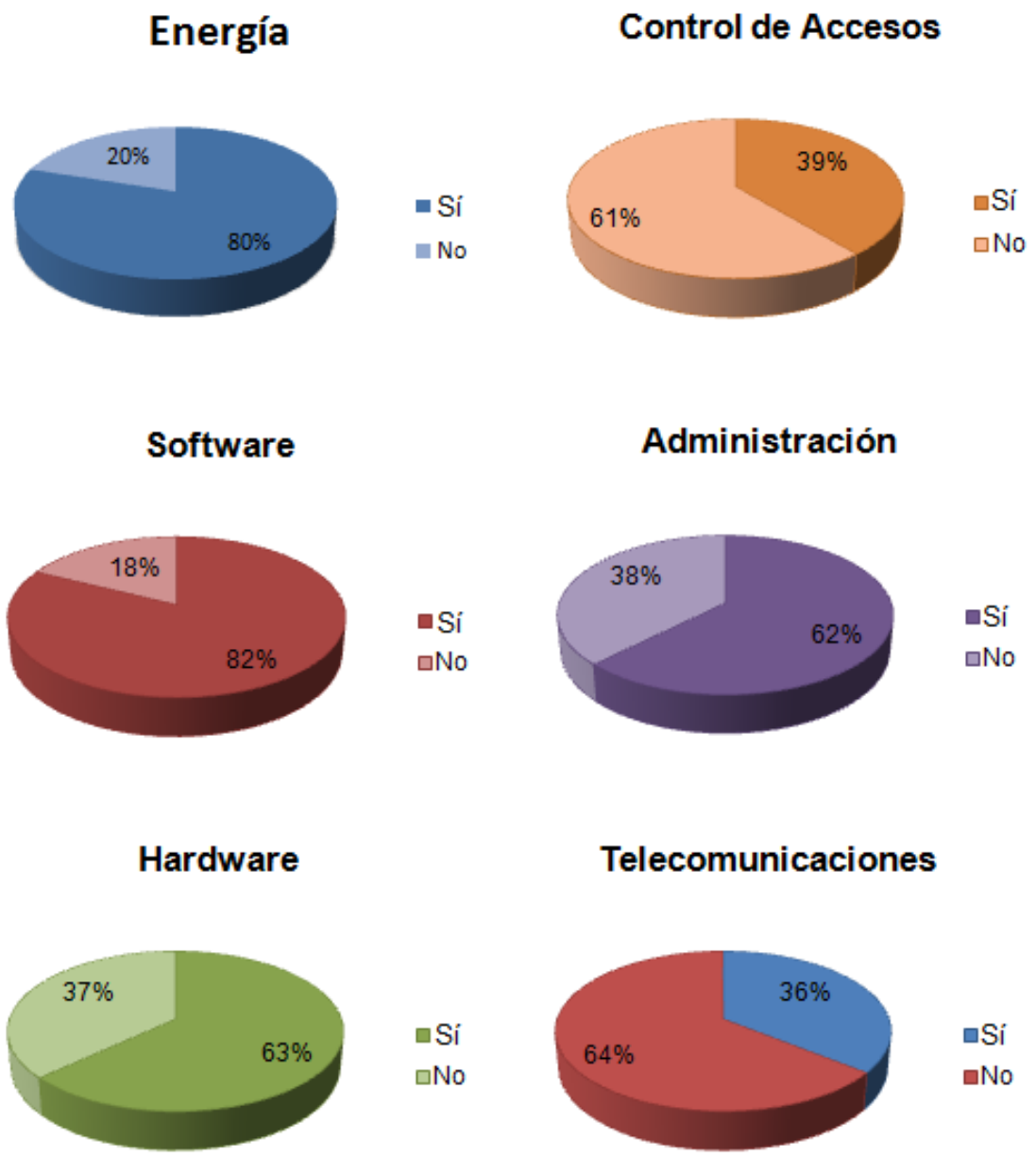
ORGANIZACIÓN 1



Gráfica 5. Porcentaje por área para Organización 1

Para la organización 1 que su mayor porcentaje está concentrado en el área de telecomunicaciones, control de accesos y hardware cuestión que no implica ausencia de áreas de oportunidad; mientras que es menor para las áreas de software, administración y energía (grafica 5) a las cuales debe poner mayor atención y tomar acciones correctivas de mejora, tomando en cuenta que no siempre estuvo mal ya que con el cambio de los cuestionarios pasó de una calificación satisfactoria a una **calificación no satisfactoria de 5.8**.

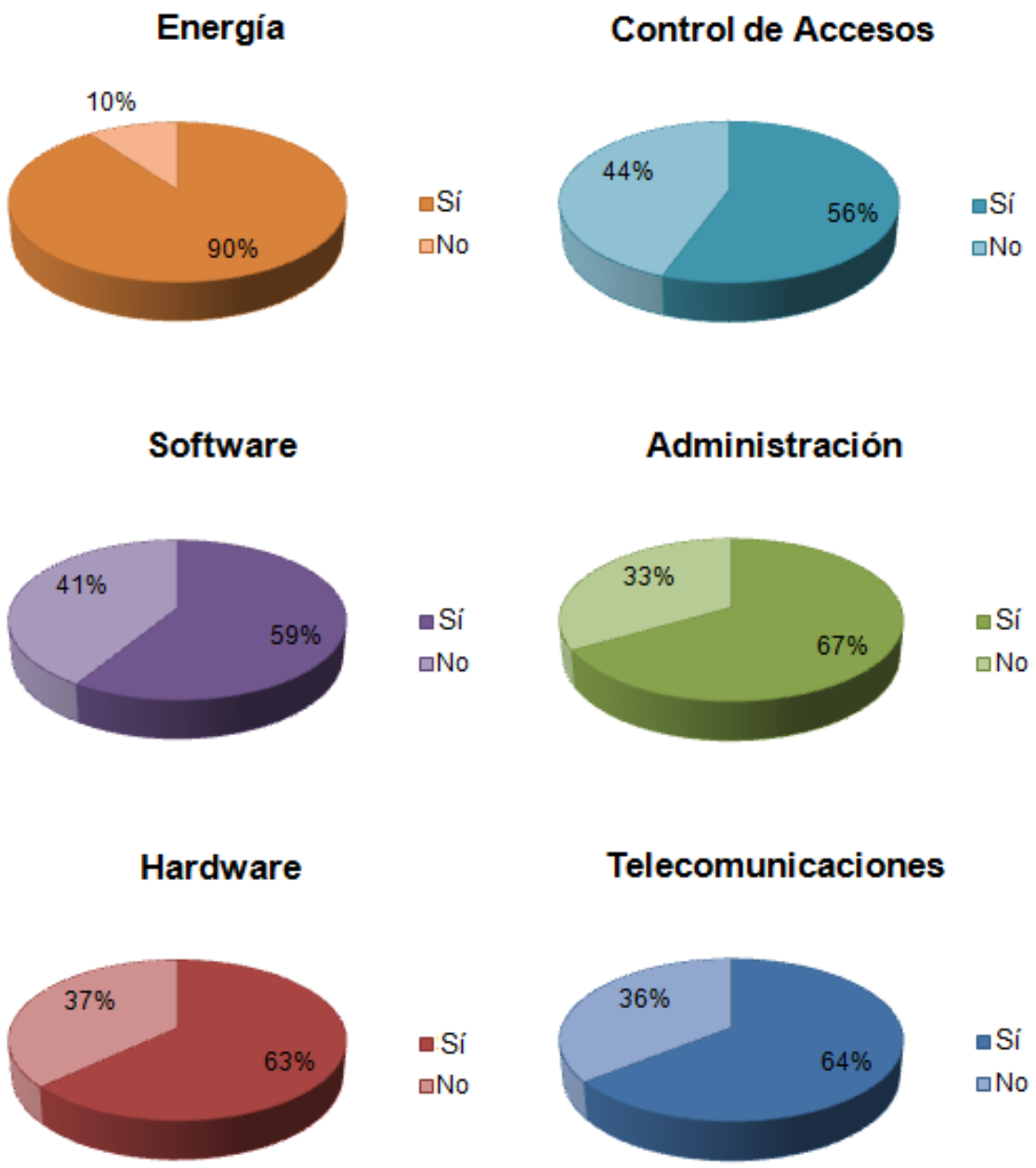
ORGANIZACIÓN 2



Gráfica 6. Porcentaje por área para Organización 2

La gráfica 6 para la organización 2 muestra un porcentaje satisfactorio en dos áreas mientras que para las cuatro restantes obtuvo un porcentaje no satisfactorio(grafica 6) lo cual implicó una **calificación no satisfactoria de 5.8**.

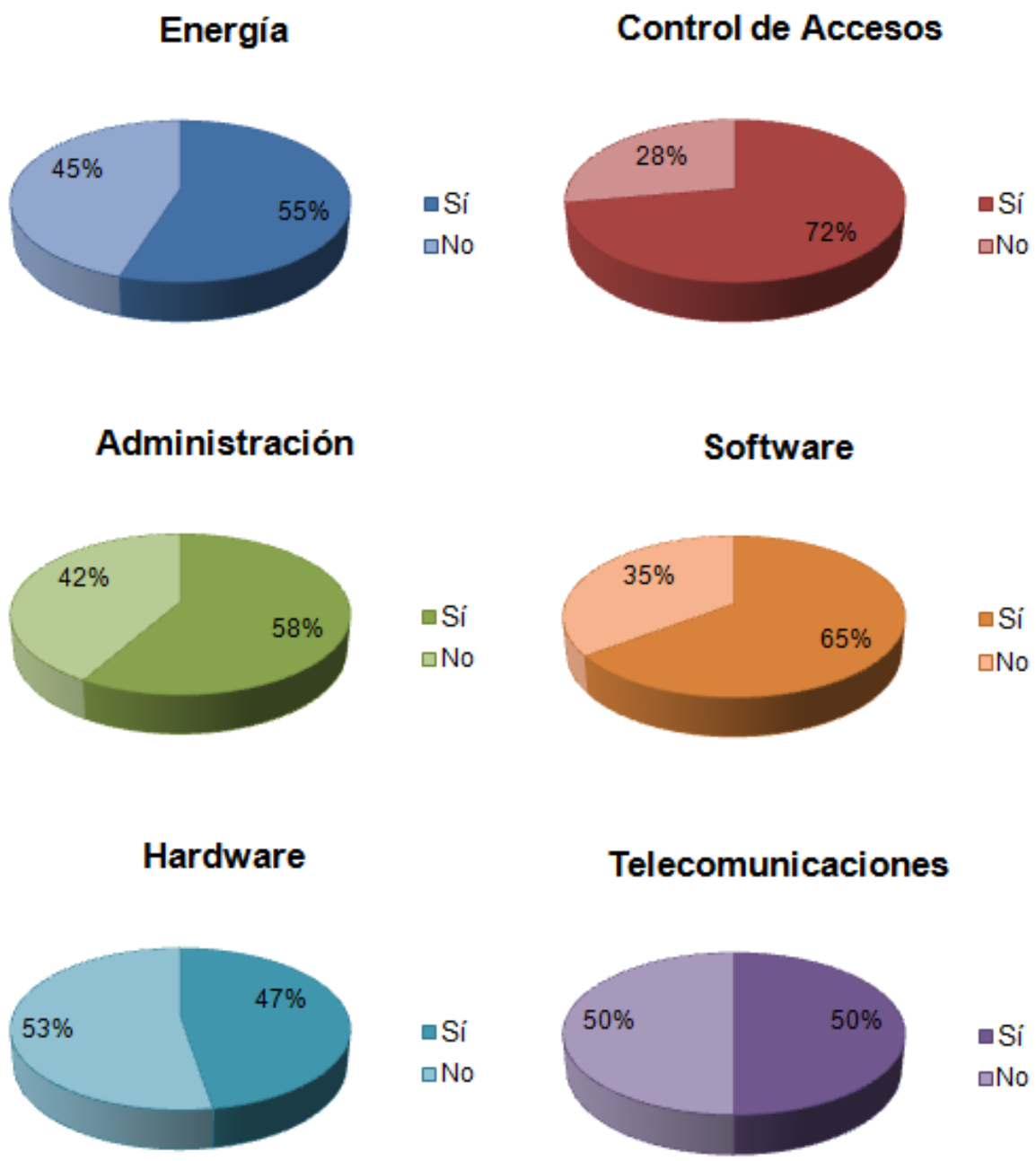
ORGANIZACIÓN 3



Gráfica 7. Porcentaje por área para Organización 3

Para la organización 3 se muestra un porcentaje satisfactorio para el área de energía y las las cinco restantes con un porcentaje no satisfactorio (grafica 7) que tambien reflejó una **calificación no satisfactoria de 6.68**.

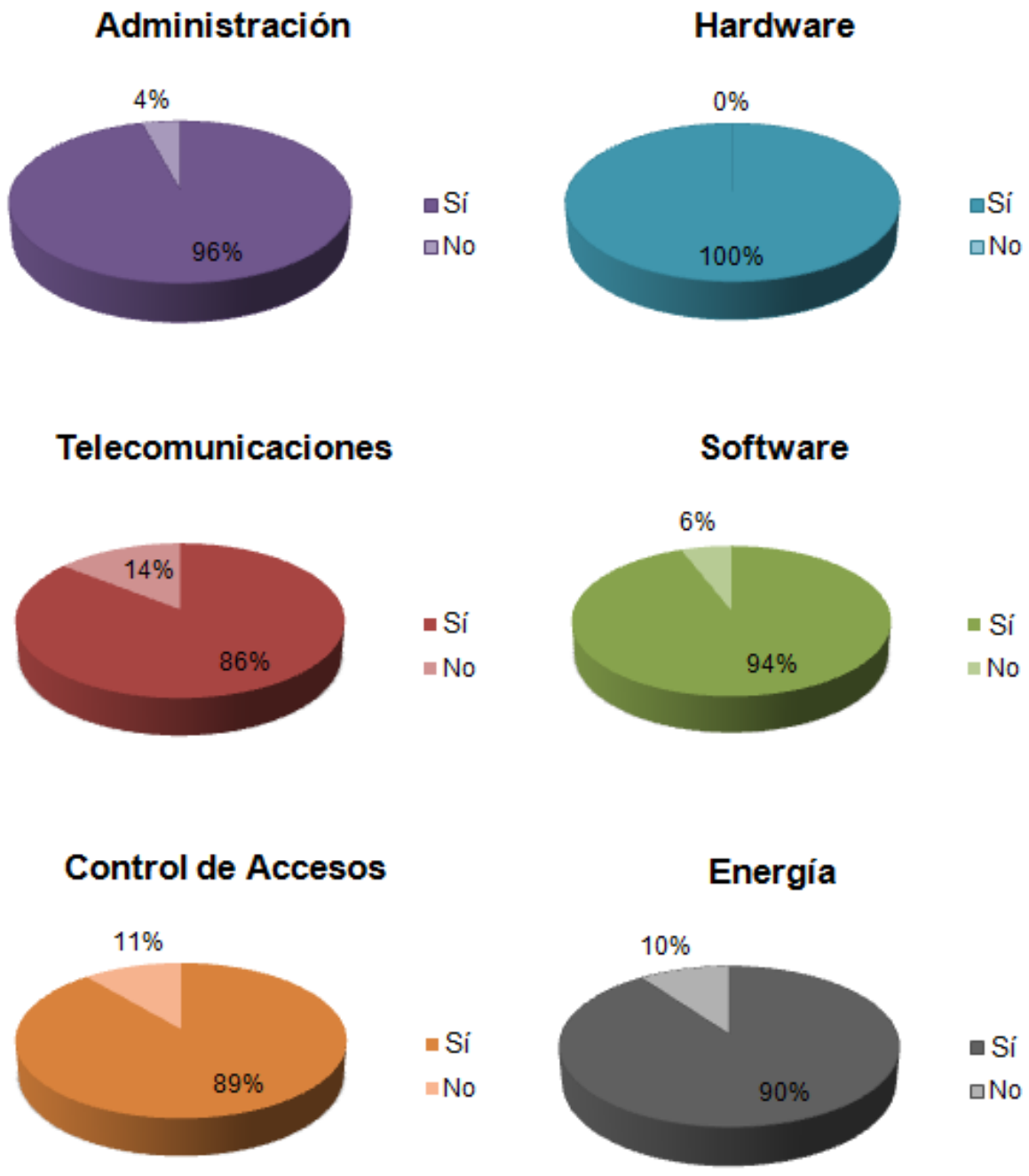
ORGANIZACIÓN 4



Gráfica 8. Porcentaje por área para Organización 4

Para la organización 4 podemos ver un porcentaje satisfactorio para el área de control de accesos mientras que para las áreas restantes cuentan con un porcentaje no satisfactorio(grafica 8) lo cual reflejó una **calificación no satisfactoria de 6.19**.

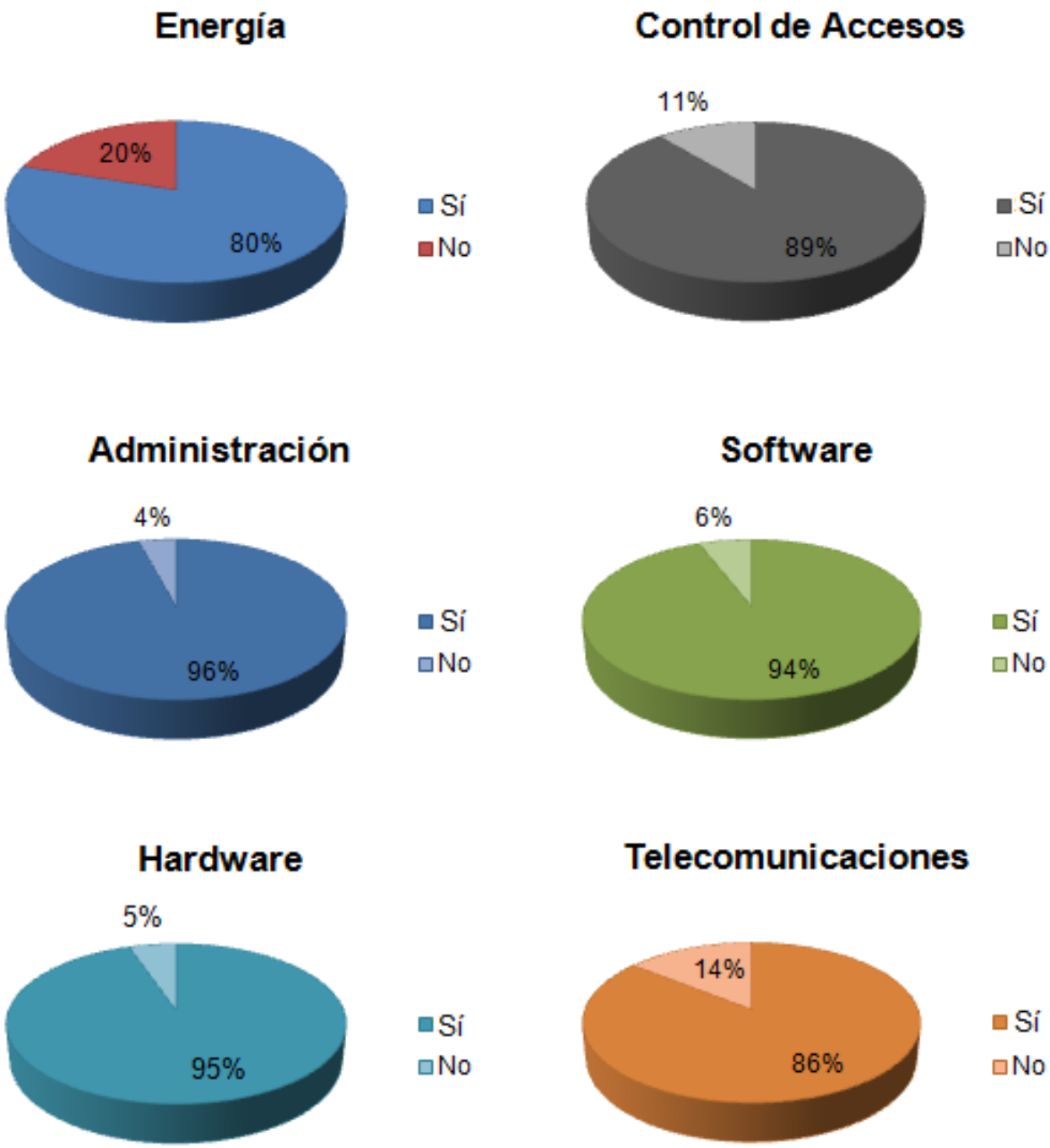
ORGANIZACIÓN 5



Gráfica 9. Porcentaje por área para Organización 5

Para la organización 5 podemos observar una distribución uniforme del porcentaje satisfactorio (grafica 9) para cada una de las áreas lo que resultó en una **calificación satisfactoria de 9.12**.

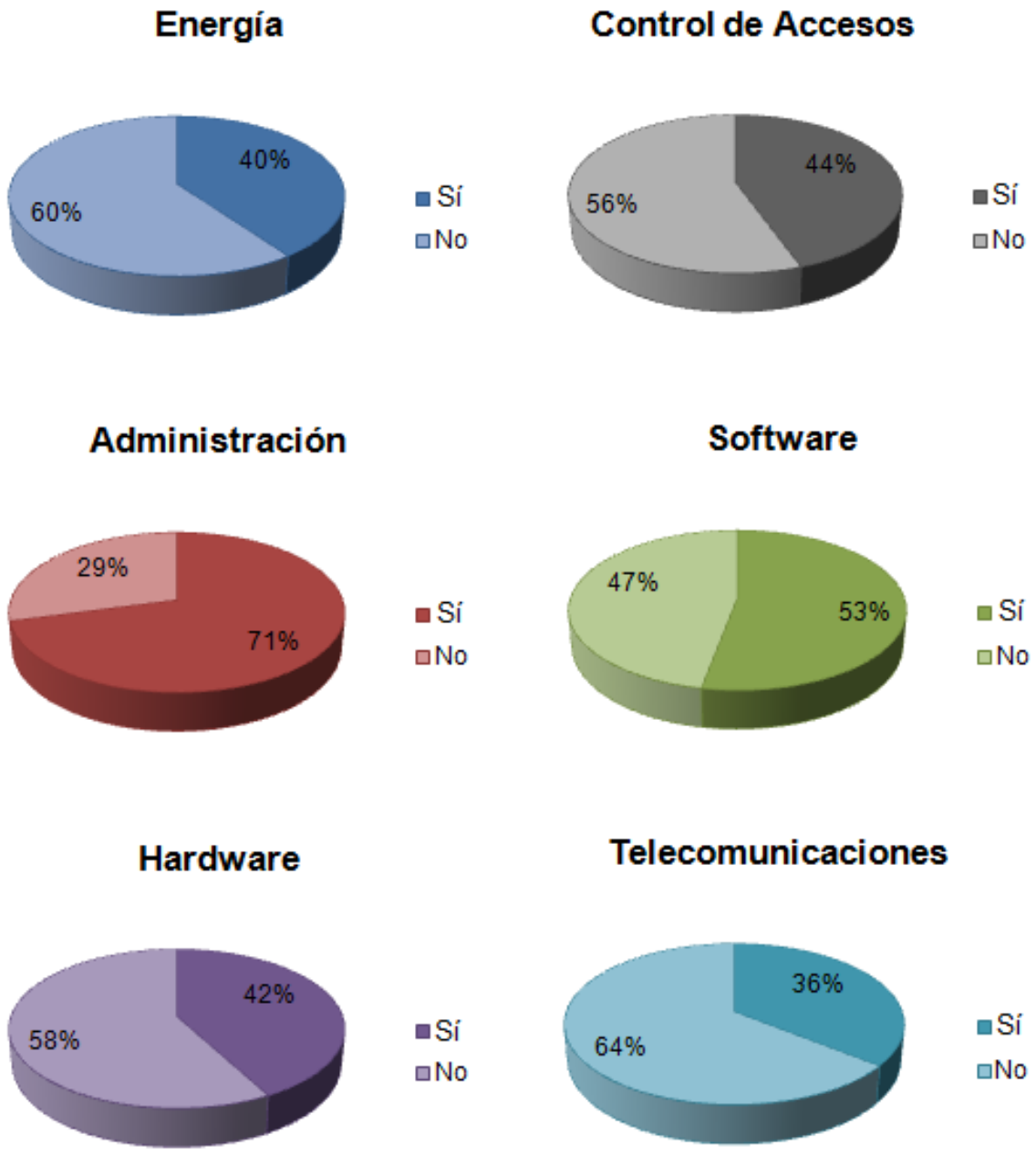
ORGANIZACIÓN 6



Gráfica 10. Porcentaje por área para Organización 6

Para la organización 6 podemos ver una distribución uniforme de porcentaje satisfactorio (grafica 10) lo cual implicó una **calificación satisfactoria de 8.94**.

ORGANIZACIÓN 7



Gráfica 11. Porcentaje por área para Organización 7

Para la organización 7 podemos ver que obtuvo un porcentaje satisfactorio solo para un área mientras que las restantes obtuvieron un porcentaje no satisfactorio (grafica 11)lo cual resultó en una **calificación no satisfactoria de 4.64**.

2.4.4 DIAGNÓSTICO GENERAL

Como resultado de nuestro trabajo de investigación, generación del método, aplicación del método y análisis de los resultados pudimos ver que solo el 30% de las áreas/organización tienen un porcentaje satisfactorio.

Con estos resultados podemos decir que en términos generales la mayoría de las organizaciones de nuestra muestra no cuentan con el perfil suficiente para poder establecer un plan de seguridad de las tecnologías de información y comunicaciones satisfactorio.

A continuación se enlistan las recomendaciones que a nuestro juicio debe contemplar cada organización para mejorar su plan de seguridad.

ORGANIZACIÓN 1

- Que la tierra física cumpla con la norma oficial(NOM-001).
- Que el cableado esté debidamente instalado.
- Identificar los cables debidamente (positivo, negativo y tierra física).
- Los contactos para el equipo de cómputo esten debidamente identificados.
- Contar con los planos de instalación eléctrica y que estén actualizados.
- Conectar los equipos de cómputo a una instalación eléctrica independiente.
- Contar con reguladores de corriente para los equipos de cómputo.
- Verificar periódicamente las cargas máximas y mínimas.
- Tener unidades de energía ininterrumpible que duren el tiempo suficiente para respaldar archivos.
- Probar el funcionamiento de las unidades de energía ininterrumpible.
- Necesario tener los paneles de control de energía eléctrica bajo llave.
- Contar con un procedimiento para la actualización del hardware institucional.
- Contar con un plan de capacitación para atención de incidentes de software, hardware, energía eléctrica y telecomunicaciones.
- Contar con un programa de monitoreo de hardware, software, energía eléctrica y telecomunicaciones.
- Contar con un directorio de proveedores en caso de una emergencia de software, hardware, energía eléctrica y telecomunicaciones.
- Contar con el equipo necesario para combatir siniestros de energía eléctica, telecomunicaciones y hardware.
- Identificar a las personas que ingresan al Site.
- Aislar el Site del resto del edificio.
- Contar con un circuito cerrado de televisión para el Site.
- Contar con la configuración institucional del hardware e identificarlo físicamente mediante algún logotipo.
- Contar con un plan para el mantenimiento preventivo.
- Contar con un plano actualizado de la ubicación del equipo de cómputo.
- Contar con inventario y configuración del software institucional, así como al menos dos copias de este.
- Contar con un procedimiento de autorización para la atención de solicitudes de soporte técnico.

- Realizar un análisis de las solicitudes.
- Contar con licencias originales del producto y pagar cuotas de mantenimiento anual para tener un mejor desempeño y respuesta.
- Contar con un plano de la instalación del cableado y del sistema de telecomunicaciones. Así mismo, que el cableado sea de fácil acceso para labores de mantenimiento.
- Que el cableado de comunicaciones este separado de la instalación eléctrica.
- Que el personal cuente con la capacitación debida para resolver los incidentes que se presenten.
- Tener un procedimiento sobre qué hacer en caso de desastres naturales.

ORGANIZACIÓN 2

- Se recomienda que la tierra física cumpla con la disposición oficial.
- Verificar periódicamente la regulación de las cargas máximas y mínimas.
- Probar periódicamente el funcionamiento del generador de corriente ininterrumpida.
- Tener un switch de apagado en caso de emergencia en un lugar visible.
- Contar con un procedimiento de actualización de software.
- Contar con un programa de monitoreo de hardware y energía eléctrica.
- Contar con un directorio de proveedores en caso de una emergencia de energía eléctrica.
- Contar con el equipo necesario para combatir siniestros de energía eléctrica, telecomunicaciones, hardware y software.
- Debe tener buenas referencias del personal de vigilancia y ver que sean confiables y verificables.
- Los colaboradores que trabajen después del horario deben justificar su estancia.
- Identificar debidamente a toda persona que ingresa a la organización y a su vez una vigilancia 24/7 para el Site, extender un formato de acceso al mismo así como hacer rondas y verificación del buen estado de los medios de seguridad.
- Aislar el Site del resto del edificio.
- Contar con una configuración institucional del Hardware.
- Contar con un procedimiento para recibir asesoría externa.
- Contar con un plan establecido para el mantenimiento correctivo.
- Tener servidores espejo.
- Tener hardware alternativo en caso de avería o fallo.
- Tener acceso restringido a los servidores.
- Tener un plano actualizado de la ubicación del equipo.
- Contar con una configuración del software institucional.
- Contar con un identificador de eficiencia en la atención de las solicitudes de soporte técnico.
- Contar con un procedimiento en caso de recibir asesoría externa.
- Tener sistemas alternativos de comunicación de datos y voz en caso de avería o fallo.
- Realizar pruebas periódicas para garantizar la calidad de los servicios de comunicación.
- Contar con un procedimiento de actualización del plano de la instalación del cableado y sistemas de comunicaciones del edificio.

- Revisar periódicamente los paneles de telecomunicaciones y protegerlo de accesos no autorizados.
- Que el cableado de comunicaciones este separado de la instalación eléctrica.
- Tener una protección física para los principales cables de conexión con el proveedor de comunicaciones.
- La red inalámbrica debe contar con un mecanismo de seguridad contra intrusos. Así mismo, que permita la conexión de los invitados a la red.

ORGANIZACIÓN 3

- Tener conectado el equipo de cómputo independiente de otras instalaciones eléctricas.
- Cumplir la normativa vigente la instalación eléctrica.
- Tener protección contra fauna nociva.
- Tener reguladores funcionales para los equipos de cómputo.
- Verificar periódicamente la regulación de las cargas máximas y mínimas.
- Tener unidades de energía ininterrumpible que duren el tiempo suficiente para respaldar los archivos.
- Probar periódicamente el funcionamiento del generador de corriente ininterrumpida.
- Tener un switch de apagado en caso de emergencia en lugar visible.
- Tener los cables eléctricos dentro de paneles y tenerlos bajo llave.
- Tener un procedimiento de mantenimiento para el Site.
- Tener un procedimiento de actualización del inventario de software, hardware, instalación eléctrica y telecomunicaciones.
- Contar con un plan de capacitación para atención de incidentes de software, hardware, energía eléctrica y telecomunicaciones.
- Contar con un programa de monitoreo de software, hardware, energía eléctrica y telecomunicaciones.
- Tener un inventario de hardware y telecomunicaciones.
- Contar con un directorio de proveedores en caso de una emergencia de software, hardware, energia electrica y telecomunicaciones.
- Contar con el equipo necesario para combatir siniestros de energía, telecomunicaciones y hardware.
- Adoptar medidas de seguridad en el Área de Informática.
- Tener un responsable de la seguridad del Site.
- Investigar a los vigilantes cuando son contratados directamente.
- Controlar el trabajo fuera del horario.
- Registrar las acciones de los operadores para evitar que puedan dañar el sistema.
- Identificar a la persona que ingresa.
- Tener vigilancia en el Site las 24 horas.
- Identificar y administrar las visitas en el Centro de Cómputo.
- Aislar el Site del resto del edificio.
- Tener un circuito cerrado de televisión que vigile el acceso al Site.
- Tener un control y archivo diario de las grabaciones del sistema de vigilancia.
- Tener un registro de todos los accesos a todas las áreas que cuenten con equipo informático.
- Capacitar al personal de limpieza para limpiar un Site.
- Contar con una configuración e identificacion del hardware institucional.

- Tener un procedimiento de registro y autorizacion de las Solicitudes de Soporte Técnico.
- Realizar el análisis de las solicitudes y tener un indicador de eficiencia.
- Contar con equipos originales y pagar cuotas de mantenimiento anual.
- Tener un procedimiento y bitacoras de la asesoría externa recibida.
- Tener un plan establecido para el mantenimiento preventivo periódico.
- Tener un plan establecido para el mantenimiento correctivo.
- Tener servidores espejo.
- Contar con hardware alternativo en caso de avería o fallo.
- Tener los servidores en un lugar con acceso restringido.
- Contar con un procedimiento de actualización del plano de ubicación del equipo de cómputo.
- Tener responsivas de usuarios.
- Contar con un inventario del software institucional. Así como, la configuración del software y tener al menos dos copias de este.
- Tener un procedimiento de registro y autorización de las Solicitudes de Soporte Técnico
- Realizar el análisis de las solicitudes y tener un indicador de eficiencia.
- Contar con licencias originales y paga cuotas de mantenimiento anual.
- Tener un procedimiento y bitacoras de la asesoría externa recibida.
- Tener un procedimiento periódico para realizar respaldos de la información sensible de manera programada.
- Tener instalado un Antivirus.
- Tener sistemas alternativos de comunicación de datos y voz en caso de avería o fallo.
- Realizar pruebas periódicas para garantizar la calidad de los servicios de comunicación.
- Contar con el plano actualizado de la instalación del cableado y del sistema de comunicaciones.
- El cableado de comunicaciones debe ser de fácil acceso para labores de mantenimiento.
- Los paneles de las comunicaciones deben ser revisados periódicamente.

ORGANIZACIÓN 4

- Tener debidamente identificados los contactos del equipo de cómputo.
- Contar con los planos de instalación eléctrica actualizados.
- Tener conectado equipo de cómputo independiente de otras instalaciones eléctricas.
- La instalación eléctrica debe cumplir con la normativa vigente.
- Tener protección contra fauna nociva.
- Tener reguladores funcionales para los equipos de cómputo.
- Verificar periódicamente la regulación de las cargas máximas y mínimas.
- Tener unidades de energía ininterrumpible que duren el tiempo suficiente para respaldar los archivos.
- Tener un generador de corriente ininterrumpida y probar su funcionamiento periódicamente.
- Tener un switch de apagado en caso de emergencia en lugar visible.
- Tener los cables eléctricos dentro de paneles y tenerlos bajo llave.

- Contar con un procedimiento de mantenimiento para el Site.
- Contar con un procedimiento de actualización e instalación del software y hardware.
- Tener un plan de capacitación para atención de incidentes de software, hardware, energía eléctrica y telecomunicaciones.
- Tener un programa de monitoreo de software, hardware, energía eléctrica y telecomunicaciones.
- Tener un inventario de hardware y telecomunicaciones.
- Contar con un directorio de proveedores en caso de una emergencia de software, hardware, energía eléctrica y telecomunicaciones.
- Contar con el equipo necesario para combatir siniestros de energía, hardware, energía elétrica y telecomunicaciones.
- Adoptar medidas de seguridad en el Área de Informática.
- Tener un responsable de la seguridad del Site.
- Investigar a los vigilantes cuando son contratados directamente.
- Controlar el trabajo fuera del horario.
- Registrar las acciones de los operadores para evitar que puedan dañar el sistema.
- Identifica a la persona que ingresa.
- Tener vigilancia en el Site las 24 horas.
- Identificar y administrar las visitas en el Centro de Cómputo.
- Aislar el Site del resto del edificio.
- Tener un circuito cerrado de televisión que vigile el acceso al Site.
- Llevar un control y archivo diario de las grabaciones del sistema de vigilancia.
- Contar con un registro de todos los accesos a todas las áreas que cuenten con equipo informático.
- Capacitar al personal de limpieza para limpiar el Site.
- Tener una configuración e identificación del hardware institucional.
- Contar con un procedimiento de registro y autorización de las Solicitudes de Soporte Técnico.
- Realizar el análisis de las solicitudes y contar con un indicador de eficiencia.
- Contar con equipos originales y pagar pagar cuotas de mantenimiento anual.
- Contar con un procedimiento y bitacoras de la asesoría externa recibida.
- Contar con un plan establecido para el mantenimiento preventivo periodico.
- Contar con un plan establecido para el mantenimiento correctivo.
- Tener servidores espejo.
- Contar con hardware alternativo en caso de avería o fallo.
- Tener acceso restringido a los servidores.
- Contar con un plano de ubicación del equipo.
- Contar con responsivas de usuarios.
- Contar con un inventario y configuración del software institucional. Asi como, tener al menos dos copias del mismo.
- Contar con un procedimiento de registro y autorización de las Solicitudes de Soporte Técnico.
- Realizar el análisis de las solicitudes y contar con un indicador de eficiencia.
- Contar con licencias originales y pagar cuotas de mantenimiento anual.
- Contar con un procedimiento y bitácoras de la asesoría externa recibida.
- Contar con un procedimiento para realizar respaldos de la información sensible de manera programada.
- Contar con un Antivirus.

- Tener sistemas alternativos de comunicación de datos y voz en caso de avería o fallo.
- Tener un plano actualizado de la instalación del cableado y sistemas de comunicaciones del edificio.
- El cableado de comunicaciones debe ser de fácil acceso para labores de mantenimiento y deben ser revisados periódicamente.
- Proteger el cableado de accesos no autorizados.
- Tener los equipos de comunicaciones en un lugar de acceso restringido.
- Tener el cableado de comunicaciones separado de la instalación eléctrica.
- Tener protección física para los principales cables de conexión con el proveedor de comunicaciones.
- Contar con un firewall para proteger la red.
- La red inalámbrica debe tener un mecanismo de seguridad contra intrusos y permitir que se conecten los invitados.

ORGANIZACIÓN 5

- Hacer pruebas periódicas al generador de corriente ininterrumpida.
- Contar con un plan de capacitación para atender incidentes de energía.
- Contar con respaldos programados.
- Revisión periódica para el área de telecomunicaciones.

ORGANIZACIÓN 6

- Identificar los cables debidamente (positivo, negativo y tierra física).
- Hacer una revision periódica de las cargas máximas y mínimas.
- Revisión y pruebas de los generadores de energía ininterrumpible.
- Contar con un plan de monitoreo de hardware.
- Contar con visitas programadas al Site.
- Contar con un indicador de eficiencia para el área de hardware.
- Contar con una copia del software institucional.
- Revisar periódicamente los paneles de comunicación.

ORGANIZACIÓN 7

- Identificar los cables debidamente (positivo, negativo y tierra física).
- Contar con los planos actualizados de la instalación eléctrica.
- Conectar los equipos a una instalación independiente.
- Contar con unidades de energia ininterrumpible.
- Verificar periódicamente las cargas máximas y mínimas.
- Contar con un switch de apagado de emergencia.
- Contar con un procedimiento de mantenimiento para el Site.
- Actualizar el inventario de software y procedimientos de instalación.
- Contar con un procedimiento de capacitación para atender incidentes de energía eléctrica.
- Realizar un monitoreo del hardware
- Contar con el equipo necesario en caso de siniestros de energía y telecomunicaciones.
- Contar con control de accesos para el área de informática.

- Identificar a los usuarios que ingresan al Site.
- Contar con cámaras de vigilancia.
- Contar con registros de accesos de los usuarios.
- Realizar rondas de verificación.
- Capacitar al personal de limpieza para limpiar el Site.
- Tener una configuración institucional del hardware.
- Contar con procedimientos de autorización para soporte técnico.
- Realizar el análisis de los datos.
- Contar con el personal suficiente para atender las solicitudes de soporte técnico.
- Realizar un mantenimiento preventivo periódico .
- Tener servidores espejo.
- Tener hardware alternativo en caso de avería o fallo.
- Tener responsivas de usuarios.
- Tener al menos dos copias del software instucional.
- Contar con procedimientos para solicitudes de soporte.
- Realizar el análisis de las solicitudes.
- Generar un indicador de eficiencia.
- Realizar respaldos programados.
- Contar con sistemas alternos de datos y de voz y probarlos.
- Contar con el plano de instalación de las telecomunicaciones.
- Que el cableado sea de fácil acceso para labores de mantenimiento.
- Revisar los paneles periódicamente.
- Tener proteccion fisica para los cables de telecomunicaciones.
- Contar con un firewal para la red.
- Tener un sistema de seguridad para la red inalámbrica.

Conclusiones

CONCLUSIONES

Las normas y metodologías investigadas son una pequeña parte de las muchas otras que se utilizan para hacer un análisis de la eficiencia de los sistemas implementados en las organizaciones, así como la gestión de los recursos informáticos.

Estas herramientas ayudan a que los usuarios confíen en la seguridad y control de los servicios de las Tecnologías de Información y Comunicaciones, incluso ayudan a disminuir costos al reducir la mala calidad de estos servicios. Así mismo, nos permiten hacer un balance de los riesgos a los que se está expuesto en el uso de las TIC's y así mejorar el desempeño en cuestiones de seguridad, eficacia, confiabilidad y privacidad dentro de la Organización.

Esta necesidad de contar con lineamientos para proteger la seguridad física y lógica de los sistemas es lo que provoco la creación y desarrollo de mejores prácticas, así como Organizaciones que generan y regulan estas normas.

Un ejemplo real es ISACA que es un organismo reconocido que cumple los estándares internacionales y que se encarga de formar auditores certificados que pasan por un estricto proceso de selección y exámenes periódicos para no perder la certificación.

Este trabajo cumplió el objetivo de obtener el diagnóstico del plan de seguridad de las tecnologías de información y comunicaciones en una organización. Se aplicó el cuestionario a PYMES y empresas grandes lo cual ayudo a ver las grandes diferencias que existen entre ellas y la prioridad que ponen ante la seguridad de su información.

Los responsables de las PYMES fueron muy accesibles en contraparte con los responsables de grandes empresas que fueron mucho más reservados y cuidadosos con la información que proporcionaban. Realmente están convencidos que su mayor activo a defender es la información y llevan a cabo en la medida de lo posible la adecuada protección de la misma.

Realmente comprobamos que más vale prevenir que lamentar algún incidente que afecte irreversiblemente a la organización. Por ejemplo, las PYMES por no tener una responsiva de usuario han perdido equipos, lo que implica una nueva inversión y por otra parte que disminuyan los equipos de reserva.

No es tan fácil el implementar y adaptarse a las normas y buenas prácticas existentes en el medio informático, ya que implica una inversión la cual muchas veces no es fácil desembolsar para las pymes por las fuertes cantidades que esto puede llegar a tener.

Sin embargo existen cuestiones tan simples como un inventario o un procedimiento de configuración de equipo que si pueden irse gestionando, lo que daría una mayor confianza a los usuarios de estas PYMES.

Podemos decir que al aplicar el cuestionario a las pymes sabemos que no obtendrán una calificación satisfactoria sin embargo les dará un panorama de los aspectos que deberán reforzar para lograr en el corto plazo tener un buen plan de seguridad.

Para la parte de investigación:

- El proyecto rebasó el alcance inicial dado que al investigar encontramos muchas más metodologías y documentación, por lo cual tuvimos que limitar el alcance.
- Los estándares internacionales pueden ser o no aplicables a nivel nacional por diferentes factores como lo son la cultura, el costo, la legislación y los usos y costumbres.

Para la preparación del cuestionario diagnóstico.

Este proyecto de investigación nos dejó muy en claro los siguientes aspectos:

- La importancia que tienen los detalles de redacción al expresar debidamente un escrito.
- Saber qué datos graficar y qué tipo de gráfica seleccionar.
- No es fácil llevar a cabo la construcción de un cuestionario en primera porque fue necesario leer muchos documentos y en segunda por lo laborioso que fue el compararlos y detectar posibles similitudes en sus alcances.
- Identificar las áreas de la organización que se relacionan con la seguridad de forma más estrecha.
- Decidir cuáles serían los puntos más importantes que se debían evaluar en una organización y cuáles no para este trabajo ya que en conjunto todo es importante.
- Saber qué preguntar, cómo preguntarlo y a quién preguntarle de manera que pudiéramos definir los tipos de respuestas del usuario para un posterior análisis.
- Contemplar los detalles para definir un criterio de evaluación y valoración adecuado. Para el criterio de valoración se obtuvo la media de las calificaciones de todas las áreas y se redondeó el valor a partir del cual se dio una evaluación satisfactoria o no satisfactoria.

Para el análisis de resultados quisimos hacer un cuestionario de diagnóstico que fuera:

- Práctico, al no ser muy extenso.
- Aplicable a cualquier organización sin importar su tamaño.
- Que fuera replicable vía web.
- Con indicadores fáciles de analizar mediante gráficas.

Glosario

GLOSARIO

- A -

ADM

Método de desarrollo de la arquitectura, del inglés Architecture Development Method,

Activos

Es un bien que la empresa posee y que pueden convertirse en dinero u otros medios líquidos equivalentes.

- B -

Benchmarking

Proceso sistemático y continuo para evaluar comparativamente los productos, servicios y procesos de trabajo en organizaciones

BSI

Agencian federal alemana para la seguridad en tecnologías de la información.

- C -

CAR

Del inglés Causal Analysis and Resolution

CC

Criterio Común, del latín Common Criteria

CM

Del inglés Configuration Management

CMMI

Integración de modelos de madurez de capacidades

COBIT

Objetivos de Control para Información y Tecnologías relacionadas.

COSO

Comité de organizaciones patrocinadoras de la comisión treadway

CSI

Perfeccionamiento continuo del servicio

CST

Cifrado y comprobación de seguridad

- D -

DAR

Del inglés Decision Analysis and Resolution.

DP

Dirección de un proyecto.

- E –

EXIN

Examination for Information Science in the Netherlands

- F -

FAQ

Preguntas frecuentes, del ingle Frecuent Asked questions.

FISMA

Del inglés federal information security management act of 2002

- G -

Gestión

Conjunto de operaciones que se realizan para dirigir y administrar un negocio o una empresa

- H -

Herramienta de Control

Son elementos de software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

- I -

ISEB

Information Systems Examination Board

ISACA

Information Systems Audit and Control Association

ITIL

Information Technology Infrastructure Library

ITGI

The IT Governance Institute

- K –

KPI's

Del inglés key Perfomance indicator

- L -

LAP

Programa de acreditación de laboratorios.

- M -

MA

Del inglés Measure and Analysis

MAAGTIC

Manual administrativo de aplicación general en materia de tecnologías de la información y comunicaciones

- N -

NIST

Del inglés National Institute standards and technology.

NVLAP

Programa nacional voluntario de acreditación de laboratorios

- O –

OID

Del inglés Organization, Innovation and Deployment.

OPF

Del inglés Organizational Processes Focus.

OPD + IPPD

Del inglés Organizational Processes Defining

Outsourcing

Es un contrato a largo plazo de un sistema de información o proceso de negocios a un proveedor de servicios externos.

OT

Del inglés Organizational Training

- P -

PI

Del inglés Product Integration.

PMC

Del inglés Project Monitoring and Control

PPQA

Del inglés Process and Product Quality Assurance

PMI

Project management institute.

- Q -

QPM

Del inglés Quantitative Project Management.

- R -

RD

Del inglés Requirements Development.

Resumen Ejecutivo

Es un informe de fácil lectura, gramaticalmente correcto y breve que presenta los hallazgos a la gerencia en forma comprensible.

REQM

Del inglés Requirements Management

RSKM

Del inglés Risk Management.

- S -

SAM

Del inglés Supplier Agreement Management

SCAMPI

Del ingles standards CMMI appraisal Methoed of process improvement

- T -

TOGAF

Esquema de arquitectura de esquema abierto

TI

Tecnologías de información

TIC's

Tecnologías de información y comunicaciones

TRM

Del inglés Technical reference model .

.

Referencias

REFERENCIAS

BIBLIOGRAFÍA

AGUILERA, Lopez Purificación. “Seguridad Informática”. Editor Editex pág. 21

CHRISSIS, Mary Beth, e tal. “CMMI, Guía para la integración de procesos y la mejora de productos”. 2ª. Ed. Pearson Educación. México: 2009. 630pp.

FONSECA, Luna Oswaldo. “Dictámenes de Auditoría, Guía para usuarios y operadores de información financiera.” 1ª. Ed. IICO. Lima: 2009, pág. 6.

GALGANO, Alberto. “Los siete instrumentos de la Calidad Total”. Ediciones Diaz de Santos, S.A., Madrid: 1995, pág. 99.

JAN Van Bon, e tal. *“Fundamentos de la Gestión de Servicios de TI basada en ITIL volumen 3”*. Edit. VHP, Holanda:2008. pág. 119, 306-309.

WHITMAN, Michael E. “Principles of Information Security” 4th ed. Information Security Professionals. USA: 2012, pp 624.

MESOGRAFÍA

http://api.ning.com/files/u2gdYg06meFYaRrQcaCxfptLmTGcy2B8wrTgigBnj7JnOKqK3ya3pQkNHSxKgyYB-dFWd0WaYHhFvTBKv9bkG8b921Boq3f*/guia_para_elaborar_politicas_v1_0.pdf
http://auditoriasistemas.com/auditoria-informatica/politicas-de-seguridad/
http://calidad-gestion.com.ar/boletin/42_acciones_correctivas.html
http://en.wikipedia.org/wiki/Firewall_%28computing%29
http://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
http://hederaconsultores.blogspot.mx/2009/09/acciones-correctivas-y-preventivas.html
http://inf-tek.blogspot.mx/2011/11/83-vulnerabilidades-informaticas.html
http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html
http://tools.ietf.org/html/rfc2196
http://www.alsemexicana.com/control-de-acceso/control-de-acceso.html
http://www.ecured.cu/index.php/Seguridad_Inform%C3%A1tica
http://www.eduteka.org/DiagramaCausaEfecto.php Diagrama de causa-efecto.
http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml
http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml
http://www.segu-info.com.ar/politicas/polseginf.htm
http://www.taringa.net/posts/ciencia-educacion/10396595/Politicas-de-Seguridad-Informatica.html

http://www.thedragoncorp.com/seguridad/seguridad01.html

CMMI
http://dspace.ups.edu.ec/bitstream/123456789/1464/4/CAPITULO%203.pdf
http://upana.edu.gt/web/upana/biblioteca-tesario/doc_view/774-t-ec3-180-p644-
http://www.monografias.com/trabajos12/coso/coso.shtml

COBIT
http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas
http://www.itera.com.mx/itinstitute/mails/chile/cobit.htm
http://www.monografias.com/trabajos38/cobit/cobit2.shtml

FIPS-200
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
http://itlaw.wikia.com/wiki/FIPS_200

IT Baseline
http://auditoria20101.wikispaces.com/file/view/ITBaselineProtectionManual.pdf

ITIL
http://books.google.com.mx/books?id=QHYs9yWDRsQC&pg=PA119&lpg=PA119&dq=ciclo+de+monitorizacion&source=bl&ots=z6Ly-jKSKW&sig=C11fk7B8TrFMDcIsULs9TjthR4U&hl=es&sa=X&ei=oWY_Up2BC4WN2gX7s4HgBQ&ved=0CEIQ6AEwAw#v=onepage&q=ciclo%20de%20monitorizacion&f=false
http://e-archivo.uc3m.es/bitstream/10016/11907/1/ITIL%20como%20base%20para%20evaluar%20la%20calidad%20del%20servicio%20en%20TI%20v2.pdf
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php
http://itilv3.osiatis.es/operacion_servicios_TI/monitorizacion_control.php
http://wiki.es.it-processmaps.com/index.php/M%C3%A9tricas_ITIL_-_KPIs_ITIL
http://www.best-management-practice.com/Knowledge-Centre/
http://www.itil.co.uk/
http://www.itil.org/en/vomkennen/itil/servicestrategy/index.php
http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

ISO/EIC 27002
http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/
http://www.sahw.com/wp/archivos/2007/07/24/iso-17799-es-ya-oficialmente-iso-27002/
ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management.

ISO/IEC 13335
http://es.scribd.com/doc/38930152/Resumen-Iso-Iec-13335
http://gestionsegura.blogspot.mx/2007/06/iso-13335-gua-para-la-gestin-de.html

ISO/IEC 15408:2005
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612
http://www.sans.org/reading_room/whitepapers/standards/common-criteria-iso-iec-15408-insight-thoughts-questions-issues_545

ISO 9000
http://www.sdpt.net/calidad/normasiso9000.htm

MAAGTIC
http://elempresario.mx/matersys/que-es-maagtic
http://www.maag-tic.com/
http://www.maag-tic.com/2010/08/administracion-de-proyectos-de-tic.html
http://www.normateca.gob.mx/NF_Secciones_Otras.php?Subtema=61#
http://www.normateca.gob.mx/NF_Secciones_Otras.php?Subtema=61#

NIST
http://scap.nist.gov/validation/index.html
http://www.everyspec.com/NIST/NIST-General/
http://www.nist.gov/index.html
http://www.nist.gov/itl/vote/upload/0612-iBeta-HB150-checklist-electronic.pdf
http://www.nist.gov/nvlap/upload/NIST-HB-150-17-2012.pdf
http://www.segu-info.com.ar/guias/nist.htm

PMBOK
http://www.slideshare.net/A_Proyectos_UCI/pmbok-5-11990086
http://www.12manage.com/methods_pmi_pmbok_es.html
http://www.marblestation.com/?p=660

PRINCE2
http://www.qrpinternational.es/index/prince-2/what-is-prince2
http://www.prince2.com/
http://www.liderdeproyecto.com/articulos/introduciendo_a_prince2.html

TickIT
http://es.wikipedia.org/wiki/TickIT
http://www.lrqamexico.com/servicios-que-ofrecemos/verificacion/158149-tickitiso-9001-software.aspx
http://www.tickit.org/scheme.htm

TOGAF
http://arquitecturaempresarialcali.wordpress.com/ea-frameworks/togaf/
http://enfoqueit.wordpress.com/2009/04/21/estandares-metodologias-y-marcos-de-trabajo/
http://es.scribd.com/doc/55777352/AREM05-TOGAF-Resumen
http://es.wikipedia.org/wiki/TOGAF
http://www.togaf.org/