UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DISEÑO DE SISTEMA DE GESTIÓN DE INCIDENCIAS INFORMÁTICAS EN DSE INGENIERÍA SAC LIMA - PERÚ

TRABAJO DE SUFICIENCIA PROFESIONAL

PARA OBTENER EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS

AUTOR:

Bach. BOGGIO CHANDUVÍ OLGA NATIVIDAD

ASESOR:

Ing. AMPUERO PASCO GILBERTO MARTÍN

LAMBAYEQUE - PERÚ
2017

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DISEÑO DE SISTEMA DE GESTIÓN DE INCIDENCIAS INFORMÁTICAS EN DSE INGENIERÍA SAC LIMA - PERÚ

Dr. Ing. Ernesto Karlo Celi Arévalo
PRESIDENTE

Ing. Oscar Efraín Capuñay Uceda
MIENBRO DEL JURADO

Mg. Ing. Juan Elías Villegas Cubas
MIENBRO DEL JURADO

Ing. Gilberto Martín Ampuero Pasco
ASESOR

LAMBAYEQUE - PERÚ
2017

INFORMACIÒN GENERAL:

Título del Trabajo de Suficiencia Profesional :

DISEÑO DE SISTEMA DE GESTIÓN DE INCIDENCIAS INFORMÁTICAS EN DSE INGENIERÍA SAC LIMA – PERÚ

Autor:

Apellidos y Nombres: Boggio Chanduví Olga Natividad

Correo: Olgaboggioch@gmail.com

Teléfono: 943362985

Asesor:

Apellidos y Nombres: Ampuero Pasco Gilberto Martín

Correo: martinampuero@hotmail.com

Teléfono: 979293176

Línea de Investigación:

Tecnologías de la Información TIC

Lugar:

Lima – Perú

Duración Estimada del Proyecto:

06 meses.

Firma de los Responsables:

_____	_____ _____Bach.
Boggio Chanduvi Olga Natividad	Ing. Gilberto Martín Ampuero Pasco
RESPONSABLE	ASESOR

DEDICATORIA

A mi madre. Por ser una persona dedicada, con principios, y la mujer más perseverante que he conocido en el transcurso de mi vida.

Gracias por tus consejos, tu tiempo, tus cuidados. Por tus deseos infinitos de verme cumplir mis metas. Gracias infinitas.

A mi padre, que aunque no ya no se encuentra presente físicamente, siempre estuvo y estará presente acompañándome en los momentos más importantes de mi vida, por su valor mostrado para salir adelante en los momentos más difíciles y sobre todo por su amor.

A mi hermano por ser un ejemplo de hermano y del cual aprendo de sus aciertos y su fuerza para salir adelante; por apoyarme siempre muchas gracias por estar en todo momento y todo el tiempo.

AGRADECIMIENTO

Agradecer principalmente a Dios por permitirme llegar a esta instancia del camino.

Expreso agradecimientos sinceros a: La Universidad Nacional Pedro Ruiz Gallo por haberme brindado una formación integral que me permitió adquirir los conocimientos y herramientas básicas para el desarrollo del proyecto que a continuación muestro.

A mis padres, hermano y familiares por el apoyo constante para seguir adelante durante toda la carrera

RESUMEN

El diseño de un nuevo sistema que debe implementarse posteriormente de manera integral en la empresa, y en ausencia de métodos y modelos a seguir, motiva la búsqueda de una metodología que se adapte a los procesos del negocio de la empresa.

El presente trabajo tiene como finalidad establecer un adecuado Sistema de Gestión de Incidencias Informáticas en la empresa DSE INGENIERÍA S.A.C., dejando establecido el diseño de los formatos y procesos a seguir para mejorar la gestión, en base enfoques teóricos de marcos de trabajo de buenas prácticas como por ejemplo ITIL entre otros, buscando cambiar la forma como el área de sistemas, gestiona las incidencias en la organización; con ello se deja las bases o lineamientos a seguir para un posterior desarrollo de un software que satisfaga la necesidad de gestión de incidencias y seguridad presente en la institución, garantizando la confidencialidad, disponibilidad e integridad de los datos, e igualmente procurando un nivel de riesgo aceptable para la organización.

ABSTRACT

The design of a new system that must be subsequently implemented comprehensively in the company, and in the absence of methods and models to follow, motivates the search for a methodology that adapts to the business processes of the company.

The purpose of this work is to establish an adequate Computer Incident Management System in the company DSE INGENIERÍA SAC, leaving established the design of the formats and processes to be followed to improve management, based on theoretical approaches to good practice frameworks such as for example, ITIL among others, seeking to change the way in which the systems area manages the incidents in the organization; This leaves the bases or guidelines to be followed for the subsequent development of software that satisfies the need for incident management and security present in the institution, guaranteeing the confidentiality, availability and integrity of the data, and also ensuring a level of risk. Acceptable to the organization.

INTRODUCCIÓN

DSE INGENIERIA S.A.C. es una empresa dedicada a la dirección de proyectos de ingeniería y construcción; con amplia experiencia en el sector de edificaciones urbanas e industriales, ubicada en la Av. Circunvalacion Nro. 202 Int. 1102 Res. Golf Los Incas – Lima.

La información es uno de los activos más valiosos que posee la empresa, debido a su importancia se requiere establecer un conjunto de medidas que permitan la gestión de los riesgos, la preservación de los activos y la continuidad del negocio.

El problema que enfrenta la empresa es una deficiencia en la atención y gestión de incidencias de los usuarios causando una demora en los tiempos de atención, esto debido a que la gestión es realizada de manera manual, además de no contar con una base de datos de errores conocidos que permita agilizar una incidencia repetida. Lo mencionado origina insatisfacción en el personal de la empresa, lo que repercute en una baja calidad del servicio por la ausencia de la priorización para la atención de incidencias, las cuales son atendidas conforme van ingresando omitiendo el grado de impacto o urgencia que estos llevan, generando que la atención de incidencias graves no sean atendidas a la brevedad posible.

El presente proyecto pretende mediante el diseño de los formatos y procesos del proceso establecer las bases del posterior desarrollo de un software para satisfacer la necesidad de gestión de incidencias y seguridad presente en la institución, garantizando la confidencialidad, disponibilidad e integridad de los datos, e igualmente procurando un nivel de riesgo aceptable para la organización.

ÌNDICE

TABLA DE ILUSTRACIONES

CAPITULO I
GENERALIDADES DEL PROYECTO

1 Descripción de la Organización

1.1. Historia

La empresa DSE INGENIERIA S.A.C. ubicado en la Av. Circunvalación Nro. 202 Int. 1102 Res. Golf Los Incas – Lima dedicada a la dirección de proyectos de ingeniería y construcción; con amplia experiencia en el sector de edificaciones urbanas e industriales

1.2. Misión

Somos una organización peruana con alcances a nivel nacional dedicada a la dirección de proyectos de ingeniería y construcción; con amplia experiencia en el sector de edificaciones urbanas e industriales.

Desde el año 2000 en condición de pioneros, venimos ofreciendo nuestros servicios aplicando como base el sistema “Construction Management (CM)”.

En DSE Ingenierías SAC, reconocemos el conocimiento como nuestro principal activo, el cual año a año venimos fortaleciendo con lecciones aprendidas, capacitación permanente y auténtica actitud de cambio, permitiéndonos hoy en día, ofrecer nuestros servicios con calidad total y confiabilidad

1.3. Visión

Ser reconocidos como la empresa de dirección de proyectos más confiable, con la mejor calidad en la entrega de sus servicios y mayor valor agregado en su gestión.

1.4. Organigrama

La empresa DSE INGENIERIA S.A.C

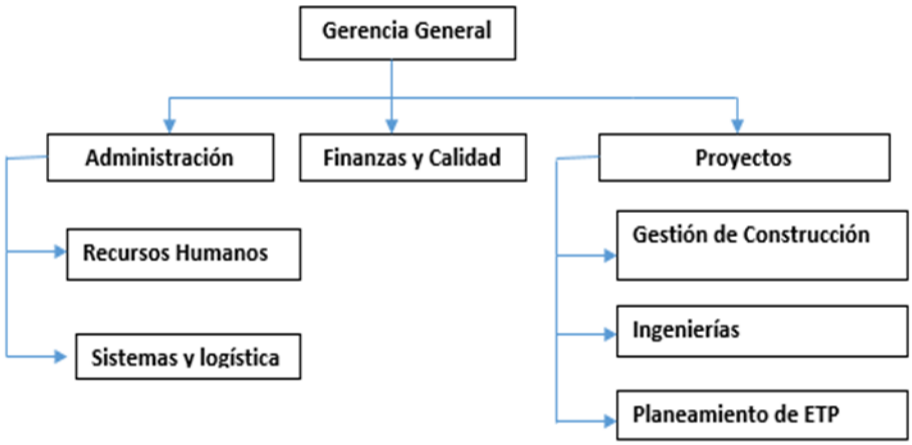

Ilustración 1 - Organigrama de la empresa

Su plana está conformada por un grupo de profesionales altamente competentes, de vasta experiencia en el sector de construcción

Ilustración 2 - Personal directivo de la empresa

2 Situación Problemática

2.1. Definición del Problema

La empresa DSE INGENIERIA S.A.C. presenta una deficiente gestión de incidencias informáticas, causando una demora en los tiempos de atención, esto es debido a que la gestión es realizada de manera manual, además de no contar con una base de datos de errores históricos que permita agilizar una incidencia repetida; por todo lo mencionado anteriormente, se origina insatisfacción en el personal al momento de realizar sus actividades utilizando las TICs como herramienta.

DSE Ingeniería SAC es una entidad privada que necesita contar con una adecuada gestión de incidencias en la seguridad de la información, que sirva como base para la implementación de un Sistema de Gestión de Seguridad de la Información.

El problema que enfrenta la empresa DSE Ingeniería SAC, es una deficiencia en la atención y gestión de incidencias de los usuarios causando una demora en los tiempos de atención, esto es debido a que la gestión es realizada de manera manual, además de no contar con una base de datos de errores conocidos que permita agilizar una incidencia repetida; lo mencionado anteriormente origina insatisfacción en el personal administrativo, financiero , ingenierías y proyectos de construcción, lo que se muestra una baja calidad en el servicio por la ausencia de la priorización para la atención de incidencias, las cuales son atendidas conforme van ingresando omitiendo el grado de impacto o urgencia que estos llevan, generando que la atención de incidencias graves no sean atendidas a la brevedad posible.

Por otro lado, no se cuenta con normas de seguridad que ayuden a proteger los activos de información, esto ha originado que se presentan diferentes incidentes de seguridad tales como la perdida de información, daño de equipos informáticos, borrado y modificación de información sensible, deterioro de activos físicos, entre otras.

Actualmente, una aplicación de correo llamada “Outlook 2010”, a través de la cual se realizan la mayor parte de las consultas. La comunicación por medio de correos electrónicos entre los trabajadores (empleados y operarios) de la empresa, cuando no se hace directamente por teléfono, conlleva estar siempre pendiente y disponible para

tratar de resolver cualquier incidencia lo antes posible. La no disponibilidad, en un momento dado, de una solución adecuada, debido a una dilación en la transmisión de la información o en la generación de respuestas por la persona responsable, con frecuencia causa una interrupción en algún proceso que puede paralizar, incluso, una parte importante de la actividad de la empresa

En DSE Ingeniería SAC, existen amenazas que afectan a los activos, entre las más destacables podemos mencionar: La pérdida de integridad de información digital, infiltración o acceso no autorizado en los sistemas, propagación de virus y software malicioso, suplantación de personal, uso de contraseñas débiles, deterioro de activos físicos, perdida de documentos, fallas de hardware, problemas de recuperación de información, perdida de documentos físicos, fallas en el Hardware, problemas de recuperación de información, problemas de denegación de servicios, problemas con ubicación en áreas susceptibles a desastres, divulgación de información, información oculta en las memorias USB, equipos dañados, entre otros.

Como respuesta a esta problemática se elabora el presente documento, el cual busca diseñar un sistema de gestión de incidencias informáticas que permita conocer las vulnerabilidades, amenazas y riesgos a los cuales están expuestos los activos, para así establecer objetivos, políticas, procedimientos y acciones encaminadas a garantizar la confidencialidad, disponibilidad e integridad de los activos de información que tiene la empresa, y de igual forma mantener el nivel de riesgo en un nivel aceptable.

2.2. Objetivos del Proyecto

2.1.1. Objetivo General

Diseñar el sistema de gestión de incidencias informáticas en la empresa DSE Ingeniería SAC – Lima.

2.1.2. Objetivos Específicos

- Estudio de documentación relacionada a la gestión de incidencias informáticas
- Análisis de la situación problemática del flujo de información en la empresa DSE Ingeniería SAC – Lima
- Definir el procedimiento para reporte y atención de incidencias informáticas
- Definir los formatos que documenten el procedimiento de atención de incidencias informáticas

2.3. Alcance del Proyecto

El proyecto se responsabiliza del diseñode formatos y el proceso para el sistema de información de gestión de incidencias informáticas en la empresa DSE Ingeniería SAC – Lima

El proyecto no se responsabiliza directamente del diseño de software para control de incidencias, más si define algunos lineamientos técnicos para su posterior implementación.

El proyecto no incluye la codificación del sistema de gestión de incidencias informáticas

2.4. Justificación del Proyecto

PARA LA INSTITUCIÓN

El proyecto se justifica debido a que su desarrollo permite a la empresa el manejode información financiera, gerencial, presupuestal, confidencial sobre los clientes (de los proyectos que se adjudican), proveedores, información sobre la actualización de cuotas, gestión de unidades de venta, contratos, fideicomisos, pedidos, facturación y cuentas corrientes con los que se trabaja. Debido al nivel de confidencialidad que requieren los datos se hace necesario plantear un conjunto de medidas para mitigar problemas de seguridad al interior de la institución

El desarrollo del presente proyecto busca satisfacer la necesidad de seguridad presente en la institución antes mencionada, garantizando la confidencialidad, disponibilidad e integridad de los datos, e igualmente procurando un nivel de riesgo aceptable para la organización, apoyados siempre en el diseño de un Sistema de gestión de seguridad de la información

PARA EL INVESTIGADOR

El desarrollo del proyecto resulta importante para el investigador porque permite la obtención de su título profesional de ingeniería de sistemas.

CAPITULO II
FUNDAMENTO TEÓRICO

1. Marco teórico

1.1. Gestión de incidencias

Definición

(Carlos, 2012)La Gestión de Incidencias tiene como objetivo resolver, de la manera más rápida y eficaz posible, cualquier incidente que cause una interrupción en el servicio.

Objetivos

Los objetivos principales de la Gestión de Incidencias son:

- Detectar cualquier alteración en los servicios TI
- Registrar y clasificar estas alteraciones
- Asignar el personal encargado de restaurar el servicio según se define en el SLA correspondiente

Esta actividad requiere un estrecho contacto con los usuarios, por lo que el Centro de Servicios debe jugar un papel esencial en el mismo

Procedimiento de gestión

- Aparición de la incidencia: el usuario detecta la incidencia y reporta emitiendo una petición de servicio

- Service Desk: es el responsable directo de la atención para la incidencia, generalmente pertenece a la dirección de TI de la organización y es el principal responsable de dar solución a la petición

- Registro y clasificación: se encarga de crear un registro de la incidencia ocurrida en la base de conocimiento; calculando para cada una de ellas prioridad y clasificándola para su asignación de personal

Ilustración 3 - Procedimiento de gestión de incidencias

- KDB: corresponde a la organización de la base de datos de conocimiento para la gestión de incidencias, la cual constituye un histórico de la información de incidencias anteriormente presentadas y los mecanismos de solución utilizados

  - Incidencia conocida: si producto de la verificación en KDB se determina que
    la incidencia ha sido anteriormente resuelta, entonces se repite el proceso utilizado.

  - Incidencia nueva: se procede de dos maneras:

- Escalado funcional: cuando se recurre a técnicos de nivel superior
- Escalado jerárquico: es necesario recurrir a los más altos directivos responsables de la organización de TI

    - Resolución y cierre: cuando se ha resuelto el incidente satisfactoriamente. Se procede a:

  - Registro del proceso en el sistema y, si es de aplicación, en la base de datos de conocimiento KDB
  - Generar una petición de cambio, de ser necesario, a la gestión de cambios

Beneficios

Los principales beneficios de una correcta Gestión de Incidencias incluyen:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio acordados en el SLA.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Una CMDB más precisa, pues se registran los incidentes en relación con los elementos de configuración.
- Y principalmente: mejora la satisfacción general de clientes y usuarios.

1.2. **ISO 27001:2013**

Definición

(Andrés, 2009)ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionarla seguridad de la información en una empresa, Este estándar ISO 27001 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Evolución

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación, es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente, en el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión, en el 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001, fue revisada y actualizada la ISO 17799, lo cual quedo como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Ilustración 4 - Total de certificados en la Norma ISO 27001

En Marzo de 2006, posteriormente surgió la ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información

Asimismo, ISO ha continuado, el desarrollo de otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.5

La última serie reciente es la publicación de las norma ISO/IEC 27001:2013, ISO/IEC 27002:2013 ambas aprobadas en la misma fecha: 25 de Septiembre de 2013.

Ilustración 5 - Evolución de la Norma ISO 27001

Los cambios que han traído la nueva norma ISO 27001: 2013 son varios, a continuación se mencionan los siguientes:

- Las acciones preventivas se reemplazaron por acciones para abordar los riesgos y oportunidades.
- Los requisitos de evaluación de riesgos son ahora más generales y se alinean con la norma ISO 31000.
- Los requisitos de la declaración de aplicabilidad son similares pero se da mayor claridad en la determinación de los controles del proceso de tratamiento de riesgos
- Mayor énfasis en el establecimiento de los objetivos, el seguimiento del desempeño y métricas.
- La norma ahora es menos descriptiva y prescriptiva.
- Da mayores libertades en la implementación.
- Propone un periodo de transición para las organizaciones ya certificadas.

Estándar

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente

Ilustración 6 - Estructura de la Norma ISO 27001

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Ilustración 7 - Alcance de la gestión de seguridad de información

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe

implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

- Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

- Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

- Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

- Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.

- Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

- Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

- Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

- Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

- Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

- Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

- Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

- Annexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

1.3. ITIL

Definición

(Bon, 2008)La Biblioteca de Infraestructura de Tecnologías de Información (o ITIL, por sus siglas en inglés) es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI

Historia

Lo que actualmente se conoce como ITIL versión 1, desarrollada bajo el auspicio de la CCTA, se tituló Government Information Technology Infrastructure Method ('Método de Infraestructura de la Tecnología de Información del Gobierno', GITM) y durante varios años terminó expandiéndose hasta unos 31 libros dentro de un proyecto inicialmente dirigido por Peter Skinner y John Stewart. Las publicaciones fueron retituladas principalmente como resultado del deseo (por Roy Dibble de la CCTA) de que fueran vistas como una guía y no como un método formal, y como resultado del creciente interés que había fuera del gobierno británico.

Muchos de los conceptos principales de gestión de servicios no surgieron dentro del proyecto inicial de la CCTA para desarrollar ITIL. IBM afirma que sus Yellow Books (A Management System for the Information Business, 'Un sistema de gestión para el negocio de la información') fueron precursores clave. (IBM, 1980)

Diferencias entre ITIL versión 2.0 y 3.0

- Integra a TI con el Negocio.
- Se focaliza en el valor al cliente y al negocio
- Plantea a la Organización de TI en una Unidad de Negocio Estratégica
- Alineación con el estándar ISO/IEC 20000
- Permite la sinergia con otras mejores prácticas (Cobit, CMMI)
- Se observa mayor consistencia en la estructura de los libros y de los procesos
- Provee más mapas de procesos
- Define de manera clara los términos: Servicio, Administración de Servicios de TI, Función, Proceso y Rol
- Detalla los roles y responsabilidades de los participantes claves en las actividades de los procesos
- Incluye Glosario y definiciones consistentes en todos los libros
- Establece las métricas para cada uno de los procesos

- Evidencia que la Administración de Servicio de TI, el Servicio y los Procesos deben estar sujetos al proceso de mejora continua (Plan-Do-Check-Act)
- Define y diferencia los siguientes roles: Administrador del Servicio, Dueño del Servicio, Administrador de la Mejora Continua y Administrador de Niveles de Servicio

Visión general de ITIL

(Tjassing, 2012)La biblioteca de infraestructura de TI (ITIL) toma este nombre por tener su origen en un conjunto de libros, cada uno dedicado a una práctica específica dentro de la gestión de TI. Tras la publicación inicial de estos libros, su número creció rápidamente (dentro la versión 1) hasta unos 30 libros. Para hacer a ITIL más accesible (y menos costosa) a aquellos que deseen explorarla, uno de los objetivos del proyecto de actualización ITIL versión 2 fue agrupar los libros según unos conjuntos lógicos destinados a tratar los procesos de administración que cada uno cubre. De esta forma, diversos aspectos de los sistemas de TIC, de las aplicaciones y del servicio se presentan en conjuntos temáticos.

Aunque el tema de Gestión de Servicios (Soporte de Servicio y Provisión de Servicio) es el más ampliamente difundido e implementado, el conjunto de mejores prácticas ITIL provee un conjunto completo de prácticas que abarca no sólo los procesos y requerimientos técnicos y operacionales, sino que se relaciona con la gestión estratégica, la gestión de operaciones y la gestión financiera de una organización moderna.

Los ocho libros de ITIL y sus temas son:

- Gestión de Servicios de TI
  - Mejores prácticas para la Provisión de Servicio
  - Mejores prácticas para el Soporte de Servicio

- Otras guías operativas
  - Gestión de la infraestructura de TI
  - Gestión de la seguridad
  - Perspectiva de negocio
  - Gestión de aplicaciones

- Gestión de activos de software

- Para asistir en la implementación de prácticas ITIL, se publicó un libro adicional con guías de implementación (principalmente de la Gestión de Servicios):
  - Planeando implementar la Gestión de Servicios

- Adicional a los ocho libros originales, más recientemente se añadió una guía con recomendaciones para departamentos de TIC más pequeños:
  - Implementación de ITIL a pequeña escala

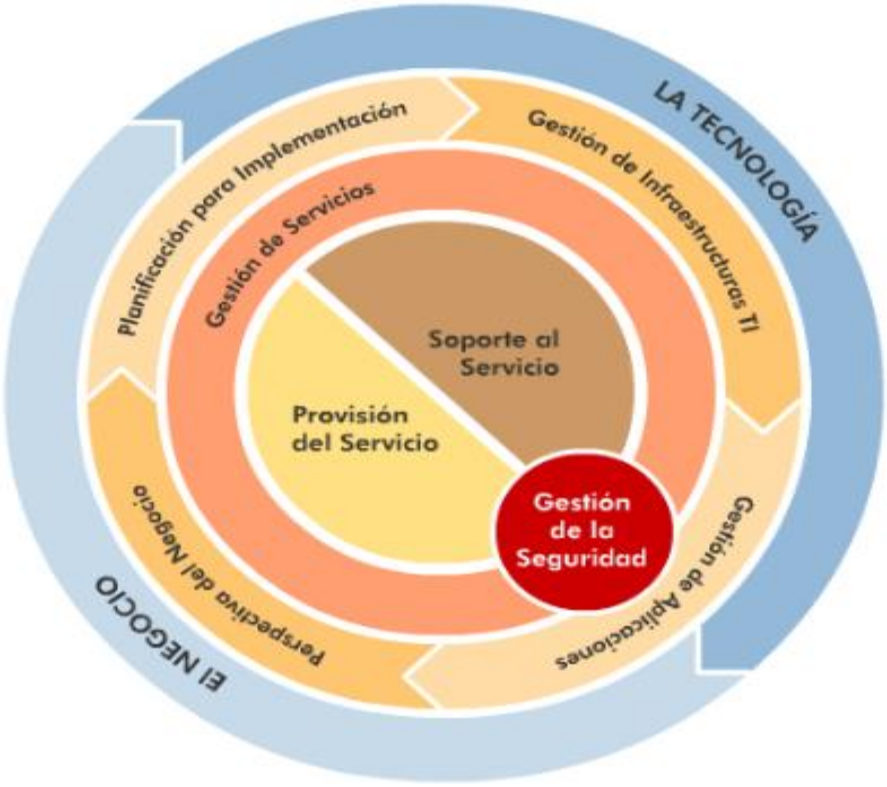

Ilustración 8 - ITIL organización del servicio

TIL v3 presenta 22 procesos, no todos son nuevos, la gran mayoría ya estaban definidos en ITIL v2 pero se describían en los otros cinco libros del marco de referencia: Planning to Implement Service Management, Business Perspective, Application Management, Security Management e ICT Infrastructure Management. Es importante comentar que los procesos fueron actualizados y se les dio consistencia, puesto que TI ha evolucionado, no fueron extraídos íntegramente.

Los procesos más conocidos de ITIL son los incluidos en los libros de Service Support y Service Delivery; los procesos de Administración de Incidentes, Problemas, Configuraciones, Cambios, Liberaciones, Niveles de Servicio, Continuidad, Disponibilidad, Capacidad, y Finanzas, así como la función del Escritorio de Servicios.

Algunos de los procesos que describe ITIL V3 con mayor énfasis y profundidad, son: Gestión del Portafolio de Servicios, Gestión del Catálogo de Servicios, Gestión de Eventos, Gestión de Solicitudes de Servicio (Request Fulfillment), Validación y Pruebas del Servicio, Soporte y Planeación de la Transición, Gestión del Conocimiento.

Ciclo de vida del servicio

El Ciclo de Vida del Servicio consta de cinco fases también llamadas disciplinas, correspondientes a los nuevos libros de ITIL:

Ilustración 9 - ITIL fases del servicio

- Estrategia del Servicio

  Se enfoca en el estudio de mercado y posibilidades mediante la búsqueda de servicios innovadores que satisfagan al cliente tomando en cuenta la real factibilidad de su puesta en marcha. Así mismo se analizan posibles mejoras para servicios ya existentes. Se verifican los contratos con base en las nuevas ofertas de proveedores antiguos y posibles nuevos proveedores, lo que incluye la renovación o revocación de los contratos vigentes. Procesos:

  - Gestión Financiera
  - Gestión del Portafolio
  - Gestión de la Demanda

- Diseño del Servicio

  Una vez identificado un posible servicio el siguiente paso consiste en analizar su viabilidad. Para ello se toman factores tales como infraestructura disponible, capacitación del personal y se planifican aspectos como seguridad y prevención ante desastres. Para la puesta en marcha se toman en consideración la reasignación de cargos (contratación, despidos, ascensos, jubilaciones, etc), la infraestructura y software a implementar. Procesos:

    - Gestión del Catálogo de Servicios
    - Gestión de Niveles de Servicios
    - Gestión de la Disponibilidad
    - Gestión de la Capacidad
    - Gestión de la Continuidad de los Servicios de TI
    - Gestión de Proveedores
    - Gestión de la Seguridad de Información
    - Coordinación del Diseño (nuevo en la versión 2011)

- Transición del Servicio

Antes de poner en marcha el servicio se deben realizar pruebas. Para ello se analiza la información disponible acerca del nivel real de capacitación de los usuarios, estado de la infraestructura, recursos IT disponibles, entre otros. Luego se prepara un escenario para realizar pruebas; se replican las bases de datos, se preparan planes de rollback (reversión) y se realizan las pruebas. Luego de ello se limpia el escenario hasta el punto de partida y se analizan los resultados, de los cuales dependerá la implementación del servicio. En la evaluación se comparan las expectativas con los resultados reales. Procesos:

- Gestión de la Configuración y Activos
- Gestión del Cambio
- Gestión del Conocimiento
- Planificación y Apoyo a la Transición
- Gestión de Release y Despliegue
- Gestión Validación y Pruebas
- Evaluación (Evaluación del cambio)

- Operación del Servicio

En este punto se monitoriza activa y pasivamente el funcionamiento del servicio, se registran eventos, incidencias, problemas, peticiones y accesos al servicio. La percepción que el cliente y los usuarios tenga de los servicios adquiridos está condicionada por la última instancia fase en la cual se ven involucrados todas las partes de la organización. En todas las otras fases del ciclo de vida, como último objeto es medir y verificar que los servicios han aportado valor a la organización, con los niveles de ANS acordados. Es primordial la entrega a satisfacción del cliente del servicio con calidad de acuerdo a lo acordado. Procesos:

- Gestión de Incidentes
- Gestión de Problemas
- Cumplimiento de Solicitudes
- Gestión de Eventos
- Gestión de Accesos

- Mejora Continua del Servicio

Se utilizan herramientas de medición y feedback para documentar la información referente al funcionamiento del servicio, los resultados obtenidos, problemas ocasionados, soluciones implementadas, etc. Para ello se debe verificar el nivel de conocimiento de los usuarios respecto al nuevo servicio, fomentar el registro e investigación referentes al servicio y disponer de la información al resto de los usuarios.

1.4. Seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente la reducción o eliminación de riesgos asociados a una cierta información es el objeto de la seguridad de la información y la seguridad

informática. Más concretamente, la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como

sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles.

Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración. Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

- La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

- La integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

- La autentificación es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

2. Términos básicos

2.1. Diseño

Proceso previo de configuración mental, "pre-figuración", en la búsqueda de una solución en cualquier campo. Utilizado habitualmente en el contexto de la industria, ingeniería, arquitectura, comunicación y otras disciplinas creativas

2.2. Incidencia

Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo

2.3. Información

Son todos los datos que maneja la empresa ya sea en forma digital o impresa. Se considera un activo de gran importancia por lo que requiere mayor protección

2.4. ISO

Organización para la creación de estándares internacionales compuesto por diversas organizaciones nacionales de estandarización

2.5. ITIL

Conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas

2.6. KDB

Base de datos de conocimiento

2.7. Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización, el riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente

2.8. Seguridad de información

Consiste en preservar la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

2.9. Service Desk

Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación

2.10. TIC

El término tecnologías de la información y la comunicación (TIC) se utiliza para referirse a cualquier forma de hacer cómputo

2.11. Vulnerabilidad

Son las debilidades que tiene una empresa, lo cual hace que se presenten amenazas a través de ellas

CAPITULO III

DESARROLLO DE LA SOLUCIÓN PROPUESTA

1. Propuesta de solución

En este punto se procederá a realizar una inspección de la situación del área de sistemas de la empresa DSE Ingenieras SAC, específicamente en el proceso de gestión de incidencias INFORMATICAS en el cómo es que se llevaba a cabo inicialmente dicho proceso, para luego proceder a la explicación de la solución propuesta que pasa por la modificación del proceso, el establecimiento de un modelo diseñado a seguir en base a normas internacionales estandarizadas como ITIL

1.1. Situación actual del área de sistemas

El área de Sistemas está liderado por el Jefe de Sistemas quien está bajo las órdenes directas del Gerente Ejecutivo, el área de Sistemas está conformado por:

- Un Jefe de Sistemas.
- Dos Técnicos de Hardware y Software.

Organigrama del área de sistemas en la Organización

Ilustración 10 - Organigrama de la empresa

Jefe de Sistemas:

El Jefe de Sistemas en DSE Ingeniería SAC, es el responsable de administrar, controlar, supervisar el correcto funcionamiento del área de sistemas incluyendo la arquitectura e infraestructura tecnológica de la empresa, es el encargado de buscar

nuevas formas de innovar con la tecnología y realizar proyectos de mejora continua en la empresa.

Técnico Hardware y Software:

Es el responsable de realizar mantenimiento preventivo y correctivo de equipos de cómputo, instalación y configuración inicial de software para usuarios e instalación y corrección de puntos de red LAN19 e inalámbrica.

Servicios de TI que proporciona el área de sistemas en DSE

Los servicios que actualmente brinda el área de sistemas se describen a continuación:

Servicios Tecnológicos del Área de sistemas - DSE	
Acceso a la red de datos	Instalación puntos de red
	Control de acceso páginas web
	Mantenimiento y gestión de Conectividad
	Configuración de red local institucional
	Configuración y acceso a la red Wireless
Servicios de apoyo a la información	Correo electrónico institucional
	Consultoría desarrollo e implementación páginas web
Apoyo al puesto de trabajo	Preparación equipos de trabajo (PC's)
	Creación de cuentas de usuario para entornos de trabajo
	Cambio de usuarios en equipos
	Instalación de Sw y licenciamiento
	Cambio de usuarios en equipos
	Mantenimiento preventivo de Sw
	Mantenimiento preventivo de Hw
	Mantenimiento correctivo de Hw
	Mantenimiento preventivo de PC’s
	Detección de virus
	Caída del servicio de internet
Distribución de SW	Distribución de S.O
	Distribución de herramientas de ofimática
	Distribución correo electrónico institucional
	Distribución de Antivirus
Otros	Asesoría para la adquisición de equipos informáticos

Autor: Elaboración Propia
Fuente: Área de Sistemas, DSE 2016

1.2. Esquema Actual de la Gestión de Incidencias Informáticas en la Empresa

El área de Soporte Técnico está conformada por dos técnicos de HW y SW que se encargan de recepcionar las solicitudes de servicio mediante llamada telefónica, Escrito, correo electrónico o petición personal, los cuales empiezan la resolución y en casos con la colaboración de otros asistentes se soluciona y hace el seguimiento hasta que se puede dar por cerrada la solicitud.

Actualmente NO se lleva el registro de los incidentes mediante formularios de soporte firmados por el usuario después de finalizado el soporte requerido y que ellos queden en conformidad.

Y en el caso de que no se pueda atender la incidencia reportada debido a que está fuera de sus parámetros, se le da la debida justificación al usuario y se da por cerrado el caso.

Descripcióndel Proceso:

Nombre: Proceso Inicial de Gestión de Incidencias Informáticas.
Objetivo: Brindar el soporte técnico necesario para la solución de incidencias que puedan presentarse en el uso de los servicios de TI, que ofrece el área de sistemas de la empresa.
Alcance: Se aplica durante todo el año y para todos los incidentes presentados en las distintas áreas de la organización.

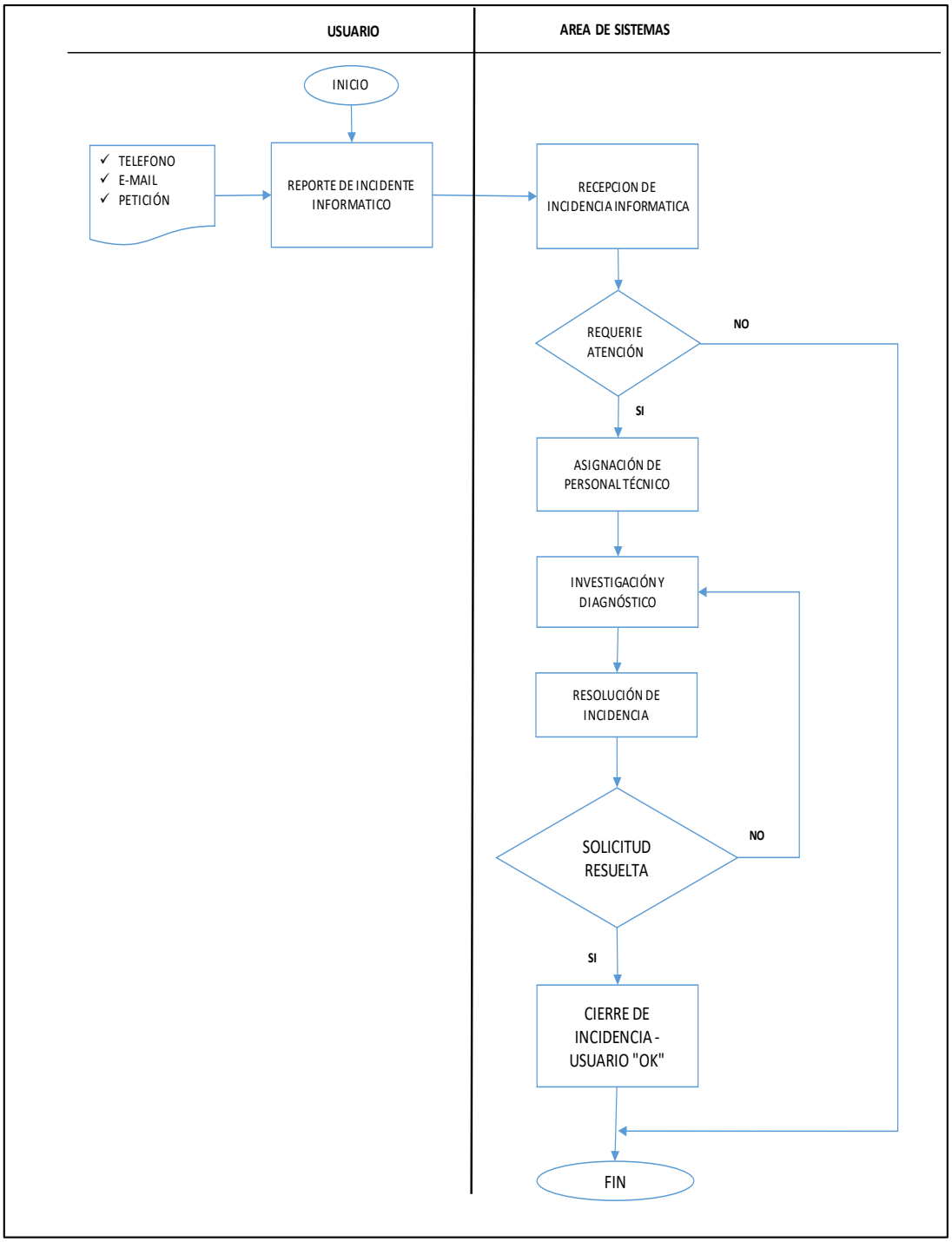

Ilustración 11 - Diagrama de Flujo del Proceso Inicial de Gestión de Incidencias Informáticas

Autor: Elaboración Propia Fuente: Área de Sistemas, DSE 2016

1.3. Problemas encontrados de TI en DSE ingeniería SAC

La técnica del cuestionario permitió saltar a la vista los puntos débiles que generan los problemas que padece el servicio de TI en DSE ingeniería SAC.

Esto permitió considerar las propuestas de soluciones a las posibles mejoras.

El siguiente es una comparativa que expone los problemas más comunes suscitados en el área de sistemas como servicio, las consecuencias que implican y propuesta de solución:

Problemas Encontrados	Consecuencias	Planteamiento de solución	Beneficios
No hay una claridad sobre el concepto de mesa de ayuda	Impide que los técnicos en cada Facultad cumplan con los servicios tecnológicos para solucionar las incidencias adecuadamente	El técnico debe estudiar los procedimientos organizados y estandarizados para atender las incidencias desde que aparecen hasta que se cierran, de acuerdo a ITIL.	Óptimo servicio a los usuarios y su satisfacción.
No mapeo de los servicios de tecnología	Impide que se detecte a tiempo las incidencias para solucionarlas.	Aplicación de herramientas para ir mapeando el estado de los equipos, usuarios y similares	Detección a tiempo de los inconvenientes suscitados.
Falta de políticas definitivamente establecidas para determinar el campo y obligaciones que deben cubrir los técnicos como profesionales.	No existencia de políticas que determinen a que deben estar dedicados los técnicos dentro de su profesión.	Definir y dar a conocer políticas claras y determinantes que lleven al técnico a tomar en consideración cuáles son sus roles como técnico informático de modo que no le permitan salir de su línea profesional y les obligue a abarcar todo lo referente a su profesionalismo en su dependencia asignada.	Evitar que olviden sus obligaciones y no pierdan el hilo en cuanto a sus conocimientos académicos y profesionales de manera que siempre se vean obligados a auto educarse y mantenerse a la par con la tecnología actual.
Falta de manejo correcto de una incidencia en todo su ciclo.	Cuando se reporta una incidencia, el técnico no siempre concluye a tiempo adecuado o no cierra la incidencia dejándola de lado.	Tener claro y estudiar cómo se gestiona o maneja una incidencia desde que inicia hasta que se cierra. El técnico debe conocer conceptos básicos de ITIL	Tiempos de respuesta óptimos. Trabajo técnico garantizado. Conformidad del usuario.
No se cuenta con auditorias periódicas de la operación de los servicios.	No se cuenta con personal determinado para hacer el control, ni autoridades encargadas de hacer auditorias que incluyan las debidas sanciones por incumplimiento	Determinar con el Director de tecnologías y autoridades pertinentes, las auditorias periódicas para obligar el cumplimiento de instrucciones, estándares, procesos, etc.	Evitar los malos procedimiento s que afecten las labores de los usuarios. Afección de la infraestructura de HW y SW por el descuido de los técnicos.
No todos los técnicos realizan en manejo de Datos adecuadament e de las unidades organizativas a su cargo de Active Directory.	Los errores generados en la creación de usuarios, unión de equipos al AD, correo institucional, dan espacio a almacenamiento de información indebida y tiempo perdido al tener que realizar correcciones	Reasignación de personal para manejo y capacitación básica de AD, para que tomen en consideración las consecuencias que conlleva el mal manejo del mismo.	Eludir errores al incluir datos de forma no cautelar. Ahorro de tiempo. Desviaciones de trabajo de técnicos que monitorean el estado.
Se pierde producción en la extensión de tiempo para el soporte por la no colaboración de los usuarios.	El mayor inconveniente es que el usuario al notificar una incidencia instantáneament e se aleja de su estación de trabajo, creyendo que cuando haya vuelto, el técnico ya debió haber reparado el suceso, sin tomar en consideración que se requiere de su colaboración.	Dar un conocimiento oficial de que cuando el usuario solicita soporte técnico, debe estar comprometido de permanecer en su lugar de trabajo antes, durante y después de la atención técnica.	Evitar retrasos en la solución de incidencias por no tener disponibilidad de contraseñas del usuario. Evitar reclamos por información no encontrada. Ahorro de tiempo.
Retraso en los pedidos de equipos, materiales y repuestos.	Demora en la reparación de los equipos, en el mantenimiento, haciendo difícil el cierre del incidente.	Establecer límite de tiempo para la adquisición de repuestos bajo prioridad por parte de las autoridades.	Ahorro de tiempo. Menos incidencias encoladas. Menos retraso en el trabajo del técnico y del usuario.

Ilustración 12 - Problemas más comunes del área de sistemas

Autor: Elaboración Propia Fuente: Área de Sistemas, DSE 2016

Algunos de los cambios que se exponen en la tabla anterior se verán reflejados con el mejoramiento de la Infraestructura y cambio en las tácticas de gestión.

1.4. Propuesta de Mejoras

Administración de servicio como una práctica

Para resolver la ausencia de conocimiento sobre el tema de Service Desk como una práctica, lo más recomendable es capacitar al técnico para que pueda interpretar los problemas con la mayor brevedad posible y dar solución, debe familiarizarse en el entorno con conocimientos suficientes y necesarios sobre servicios TI a nivel ITIL, de modo que pueda ser un especialista en atención de Service Desk y capaz de manejarse dentro de las siguientes funciones:

- Soporte en programas informáticos.
- Implantación y mantenimiento de software o Mantenimiento de bases de datos de clientes o correo.
- Servidores y redes.

Esto le permitiría realizar una mejor administración de los servicios que debe monitorear constantemente y principalmente mejorar el tiempo de respuesta hacia los usuarios a su vez brindándole un trabajo más limpio.

1.5. Propuesta de mejora del proceso de gestión de incidencias en la empresa DSE ingeniería SAC

Establecimiento del Nuevo Proceso de la gestión de incidencias.

En este punto se define establecer o generar una mesa de ayuda que sea el punto de contacto del área de sistemas o informática con los usuarios de la empresa de las diversas gerencias.

Diseño del Servicio (mesa de ayuda)

El Diseño del Servicio se encargará de crear nuevos procesos o modificar los existentes para su incorporación al catálogo de servicios y su paso al entorno de producción.

El Diseño del Servicio debe seguir con los estándares de calidad adoptados y aporten valor a los usuarios de la empresa.

Para el diseño del servicio se propone lo siguiente:

Mejorar la “Asistencia Técnica” en la empresa ya que presenta las siguientes debilidades:

- No se lleva un adecuado registro de las incidencias que se van atendiendo, los especialistas o técnicos al finalizar el día registran en un Excel sólo las incidencias más resaltantes que se le han presentado con lo cual el coordinador del área no cuenta con información completa.
- Los especialistas y/o técnicos no comparten información con respecto a la resolución de incidencias conocidas.
- Los especialistas técnicos no llevan un control adecuado de los equipos a los cuales hacen cambio de piezas.

Gestión de Incidencias:

Proceso de mejora Cuando se detecte o el técnico sea comunicado de un incidente, este será el procedimiento que se propone a seguir:

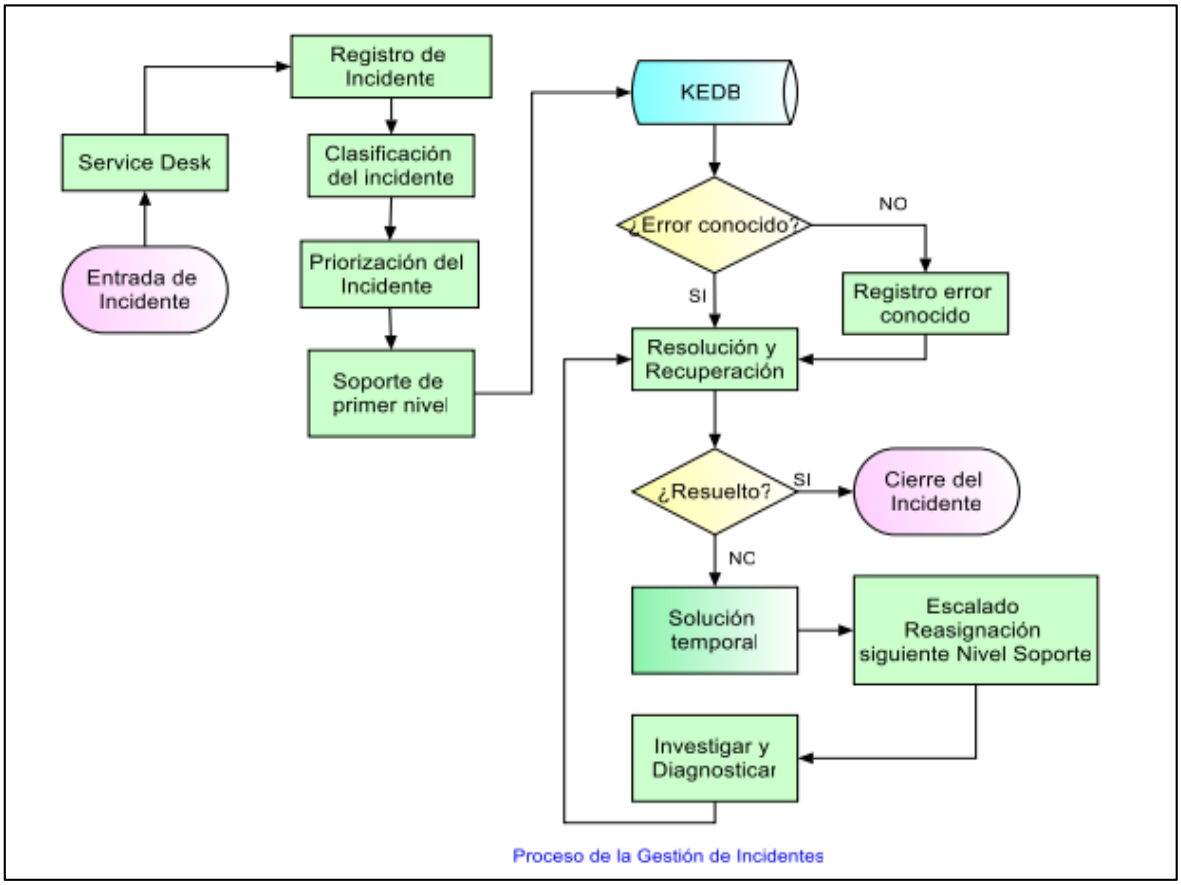

Ilustración 13 - Diagrama de Flujos – Gestión de Incidencias

Autor: Elaboración Propia Fuente: Área de Sistemas, DSE 2016

Proceso	Descripción
Service Desk	Será el encargado de tomar la notificación y encaminar el incidente para que se inicie su solución
Detectar y Registrar la Incidencia	Se realizará por el Service Desk la primera fase de soporte. De acuerdo a parámetros precisos se registra los datos y condiciones del incidente, se pone en conocimiento a los especialistas de soporte y empieza la gestión de la solicitud del servicio.
Clasificar la Incidencia, priorizar y asignar a soporte de primer nivel	Se identifica cuál es la causa del incidente generado, se da una priorización a la incidencia y envía a soporte para su solución, para ello busca en la KEDB y si no se encuentra registrar el error conocido, se soluciona si no se puedo realizar, se da una primera solución (workaround), tomando en su efecto la atención de forma urgente, y se recomienda registrar la priorización en el SLA.
Escalar	Se realiza cuando en la línea de soporte en la que se encuentra el incidente, los acuerdos de nivel de servicio no permitieron resolverlo. El escalado es funcional (horizontal se necesita conocimiento) o jerárquico (vertical -> se necesita más autoridad)
Investigar y diagnosticar	Si no se encuentra en KEDB una incidencia similar, los técnicos de soporte agrupados escalarmente; de acuerdo a cierta especialización, tiempo y recursos, actúan ante el hecho para encontrar una solución, se produce el escalamiento hasta encontrar la solución
Resolución y Recuperación	Se utiliza el conocimiento almacenado en el KEDB o que haya surgido durante la fase de investigación para solucionar el problema. O se resuelve la incidencia satisfactoriamente o se genera un RFC
Cerrar la Incidencia	Luego de solucionado se comunica al usuario y se oficializa el registro en la KEDB= Known Error Database

Ilustración 14 - Cuadro de Descripción de Procesos Gestión Incidencias, Área de Sistemas

Autor: Elaboración Propia Fuente: Área de Sistemas, DSE 2016

Ante la descripción del proceso que deben seguir los técnicos para cumplir con la adecuada gestión de una incidencia se expone quienes deben realizar las tareas y sus funciones

Roles y Responsabilidades Gestión Incidencias

Las funciones principales que se deben tomar en consideración para la gestión de Incidentes son:

- Ejecutar el rol de gerente de proceso para gestión de incidente (gerente de incidentes).
- Planear y gestionar el soporte para los procesos y herramientas de gestión de incidente.
- Coordinar las relaciones entre la gestión de incidente y los demás procesos de gestión del servicio.
- Manejar el proceso de gestión de incidente en forma efectiva y eficiente.
- Producir información relevante para la gestión de incidente.
- Administrar el trabajo del personal de soporte de incidentes de primera y segunda línea.
- Desarrollar y mantener sistemas de gestión de incidente, procesos y procedimientos o Manejar incidentes graves.
- Desarrollar y mantener procedimientos y el proceso de gestión de incidente. Registrar el incidente, clasificarlo adecuadamente y darle el direccionamiento apropiado para su correcta y pronta solución es el objetivo principal que se quiere cumplir en este proceso.

TAREA	ENCARGADO	FUNCIONES
Detección del Incidente	Usuario de TI, Operador de Service Desk	Es quién inicia el proceso desde el momento que detecta y notifica
Registro de Incidente	Operador de Service Desk	Registrar datos y condiciones del incidente, y pone en conocimiento a los especialistas de soporte y gestiona la solicitud del servicio.
Clasificación y Soporte de Primer Nivel	Operador de Service Desk	Identificar cual fue la causa del incidente dando una solución temporal.
Consulta KEDB	Operador de Service Desk	Buscar registros de anteriores incidencias, para ayudar a la solución de la actual.
Investigación y Diagnóstico	Operador de Service Desk	Si no se solucionó en primer nivel se diagnostica y de ser necesario escala
Escalamiento	Gestor de Incidentes	Revisar los SLA y si no se resolvió, escalar al siguiente nivel.
Resolución y Recuperación	Operador de Service Desk	Solucionar el problema con lo investigado
Registro de solución y Cierre Incidente	Operador de Service Desk	Documentar y registrar la incidencia, verificar que todo el proceso haya sido correcto y cerrar.

Ilustración 15 - Cuadro Roles y funciones Gestión de incidencias

Autor: Elaboración Propia Fuente: Área de Sistemas, DSE 2016

Para el caso del Área de Sistemas el Gerente de Service Desk será el mismo que hará las veces de (Gestor de Incidentes), con apoyo de un equipo de trabajo atenderán el proceso, ya que gestionarán y planificarán los procedimientos encargándose de cumplirlos

Matriz RACI Gestión Incidencias Los roles se llevarán de acuerdo a la siguiente matriz RACI de asignación

.

ENCARGADO / ACTIVIDAD	Gestor de Incidentes	Operador de Service Desk	Usuario TI
Detección y Notificación	A	I	R
Registro de Incidente	C/A	R	I
Clasificación y Soporte de Primer Nivel	C/A	I/R	
Investigación y Diagnóstico	C/A	R	C/I
Escalamiento	C/A	I/R	I
Registro de solución y Cierre Incidente	C/A	I/R	I

Ilustración 16 - Matriz RACI Gestión de Incidencias

Autor: Elaboración Propia

1.6. Impacto y Priorización Gestión Incidencias:

Impactos que causan los incidentes dentro de la organización

IMPACTO	CAUSA-EFECTO
Bajo	Paraliza temporalmente el trabajo del usuario.
Medio	Afecta el flujo de trabajo de la unidad administrativa.
Alto	Afecta la productividad de la organización

Ilustración 17 - Impacto de incidentes en la empresa

Autor: Elaboración Propia

Priorización de atención de los incidentes en la organización

PRIORIDAD	CAUSA-EFECTO
Baja	No afecta el flujo de trabajo de la unidad administrativa y se puede atender mesuradamente.
Media	No afecta la productividad de toda la organización pero requiere de atención prudente.
Alta	Afecta la productividad, requiere una solución inmediata.

Ilustración 18 - Prioridad de atención de incidentes

Autor: Elaboración Propia

Plantillas de Registros para la Base de Conocimientos Plantilla de Registro de Solicitud de Servicio

Un ejemplo de cómo se recomienda que se deben registrar las solicitudes de servicio, se muestra a continuación:

Plantilla Registro solicitud del servicio

ID de solicitud de servicio	Origen	Fecha y hora		Detalles de solicitud de servicio	
		Fecha	Hora	Categoría de solicitud de servicio	Persona solicitante
2015_1	*Telf.*	*01-12-15*	*4:55:00 PM*	*Solicitud de recursos de TI*	*Apellido, Nombre 10*

Ilustración 19 - Plantilla de registro de solicitud

Plantilla de Registro de Errores Conocidos

Los errores conocidos se generan en base a los siguientes aspectos:

Problema + Causa raíz + Solución temporal = Error Conocido

Ilustración 20 - Plantilla de registro de errores conocidos

Una de las varias maneras óptimas de registrar un error conocido se recomienda a continuación:

Plantilla Registro Error Conocido Registro del error conocido

Número del error Conocido	EC 1
Fecha de creación	01-12-2015
Estado	Para aprobar

Lista de errores conocidos

Número del error Conocido	Fecha de creación	Estado			
EC1	01-12-2015	Para aprobar			

Ilustración 21 - Listado de errores conocidos

Consejo: Registre todos los errores conocidos.

El error conocido asume que existe un problema, como también que se conocen una causa raíz y una solución temporal.

Plantilla de registro de Incidentes Un ejemplo de cómo se recomienda que se deben registrar los incidentes, se muestra a continuación:

ID de incidente	Origen	Fecha y hora		Datos del Usuario	
		Fecha	Hora	Nombre	Ubicación/Area
2015_1	Telf.	01-12-15	4:55:00 PM	Apellido, Nombre 5	Ubicación 1/ DGF / Departamento presupuesto
		05-12-15	10:45:00 AM		
		05-12-15	11:28:00 AM		

Ilustración 22 - Plantilla de registro de incidentes

Plantilla de Registro de Problemas

Un ejemplo de cómo se recomienda que se deben registrar los problemas, se muestra a continuación:

ID de Problema	Origen	Fecha y hora		EC (CI's)	Urgencia (medir en escala 1-5)	
		Fecha	Hora			

Ilustración 23 - Plantilla de registro de problemas

Si los registros de solicitudes de servicio, incidentes y problemas se hacen adecuadamente, y los procesos se siguen bajo mejores prácticas, la KEDB tendría una estructura organizada que permita disminuir óptimamente los tiempos de respuesta que actualmente maneja el área de Sistemas de la organización, porque se haría más fácil la tarea de hacer consultas de los errores conocidos para resolver futuros inconvenientes.

CONCLUSIONES

1. Se analizaron como marcos normativos relacionados a la gestión de incidencias informáticas la Norma ISO 27001-2013 y el conjunto de buenas prácticas de ITIL versión 3.0

2. Producto del análisis de la situación problemática del flujo de información en la empresa DSE Ingeniería SAC se determinó que ésta a pesar de contar con un área de sistemas de información, no contaba con políticas de gestión de incidencias, lo cual constituía un serio riesgo para la institución

3. Se definió el procedimiento para reportar y atender las incidencias informáticas que se presenten, de la siguiente forma: la incidencia es reportada al Service Desk, el cual registra la incidencia, la clasifica y prioriza. Luego evalúa en su base de conocimiento (KDB) si es incidencia conocida, de ser procede a dar solución, caso contrario investiga y diagnostica, aplicando una solución temporal hasta resolver la incidencia de forma permanente

4. Se definieron plantillas como formatos para documentar el procedimiento de atención de incidencias informáticas, entre ellas: plantilla de registro de solicitud, de registro de errores conocidos, de registro de incidentes y de registro de problemas

RECOMENDACIONES

- Se recomienda ante la ocurrencia de la incidencia recopilar información histórica que permita incrementar la base de datos de conocimiento KDB

- Se recomienda incorporar poco a poco al equipo informático de control de incidencias miembros de RR.HH., marketing, legal y directivos, asegurando de esta manera un equipo multidisciplinario.

- Se recomienda distribuir periódicamente información de emergencia a fin que los usuarios conozcan a quien acudir. Se debe decidirel método de comunicación a emplear y comunicar los detalles a todas las personas afectadas.

BIBLIOGRAFÍA

Andrés, A. (2009). *Guia de aplicación Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para PYMES.* España: AENOR ediciones.

Bon, J. v. (2008). *Estrategia del servicio basada en ITIL V3.* EEUU: Van Haren.

Carlos, F. S. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.* España: AENOR ediciones.

IBM. (1980). *A Management System for the Information Business. White Plains.* Nueva York: IBM.

Tjassing, R. (2012). *Fundamentos de ITIL V3.* EEUU: Van Haren.