

UNIVERSIDAD DON BOSCO



VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN

“Modelo de buenas prácticas TIC para micro y pequeña empresa del El Salvador”.

PARA OPTAR AL GRADO DE

Maestro en Arquitectura de Software

ASESOR:

Iván Orlando Alvarado Niño

PRESENTADO POR:

Emerson Francisco Cartagena Candelario

Dennis Antonio Pérez Escobar

Héctor Alexander Valladares Pérez

PRESTADO POR 3 DÍAS

BIBLIOTECA A. C. UDB

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Agosto 2019

UNIVERSIDAD DON BOSCO



VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN

“Modelo de buenas prácticas TIC para micro y pequeña empresa del El Salvador”.

PARA OPTAR AL GRADO DE

Maestro en Arquitectura de Software

ASESOR:

Iván Orlando Alvarado Niño

PRESENTADO POR:

Emerson Francisco Cartagena Candelario

Dennis Antonio Pérez Escobar

Héctor Alexander Valladares Pérez

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Agosto 2019

Contenido

Introducción.....	5
1. Capítulo I. Planteamiento del problema	7
1.1. Descripción del problema.....	7
1.2. Antecedentes	8
1.3. Objetivos	10
1.3.1. Objetivo general	10
1.3.2. Objetivos específicos.....	10
1.4. Justificación.....	11
1.5. Delimitación.....	11
1.5.1. Alcances	11
1.5.2. Limitaciones	12
2. Capítulo II. Estado del arte.....	12
2.1. Definición y características de las micro y pequeña empresa	12
2.2. COBIT	14
2.2.1. ¿Qué es?	14
2.2.2. Características.	16
2.2.3. Principios.....	17
2.2.4. Procesos.....	19
2.3. ITIL	21
2.3.1. ¿Qué es?	21
2.3.2. Descripción de las fases del marco de trabajo.....	23
2.3.3. Estrategia del servicio	25
2.3.4. Diseño del servicio	26
2.3.5. Transición del servicio	27
2.3.6. Operación del servicio.....	29
2.3.7. Mejora continua del servicio	30
2.4. Seguridad de Información	31
2.4.1. Concepción de la seguridad de Información	31
2.4.2. Estándares de seguridad de información	35
3. Capítulo III. Metodología de la investigación.....	38
3.1. Tipo de investigación	38

3.2.	Unidades de análisis	38
3.3.	Sujeto de estudio	39
3.4.	Variables y su medición	39
3.5.	Procedimiento y análisis.....	40
4.	Capítulo IV. Resultados	41
5.	Capítulo V. Modelo de buenas prácticas.....	44
6.	Capítulo VI. Conclusiones y recomendaciones.....	44
	Anexos	53
A.1	Instrumentos de medición	53
A.1.1	Instrumento 1	53
A.1.2	Instrumento 2.....	54
A.1.3	Instrumento 3.....	55
A.1.4	Instrumento 4.....	56
A.1.5	Instrumento 5.....	57
A.1.6	Instrumento 6.....	58
A.1.7	Instrumento 7.....	59
A.1.8	Instrumento 8.....	60
A.1.9	Instrumento 9.....	61
A.1.10	Instrumento 10.....	63
A.1.11	Instrumento 11	64
A.1.12	Instrumento 12.....	65
A.2	Instrumentos de medición completados	66
A.2.1	Instrumento 1.....	66
A.2.2	Instrumento 2.....	72
A.2.3	Instrumento 3.....	76
A.2.4	Instrumento 4.....	79
A.2.5	Instrumento 5.....	91
A.2.6	Instrumento 6.....	101
A.2.7	Instrumento 7.....	117
A.2.8	Instrumento 8.....	119
A.2.9	Instrumento 9.....	120
A.2.10	Instrumento 10.....	129
A.2.11	Instrumento 11	161

A.2.12 Instrumento 12.....	186
A.3 Modelo de buenas prácticas	192

Introducción

El propósito de este trabajo de graduación surge del poco aprovechamiento que hacen las micro y pequeñas empresas de las metodologías de tecnologías de información y comunicaciones (TIC), ya que se tiene la creencia que estas solo pueden ser utilizadas por la mediana y gran empresa.

Con el objetivo de elaborar un modelo de implementación de metodologías TIC en la micro y pequeña empresa, se estableció utilizar herramientas que contengan las mejores prácticas de TIC y seleccionar aquellas que encajen con las propiedades que describen a las micro y pequeña empresa, de esta manera se contarán con las más apropiadas y que no impliquen costos excesivos o un impacto negativo a los negocios que estas realizan.

El trabajo de graduación se dividió en cinco etapas: la primera etapa consistió en la construcción de la problemática, planteamiento de objetivos, limitaciones y justificación. La segunda constituyó la revisión bibliográfica de metodologías TIC como: COBIT, ITIL y la norma ISO 27001, a fin de identificar los lineamientos comunes entre ellas. Como siguiente etapa, la especificación metodológica, la cual permitió la construcción de instrumentos para sistematizar la información y posteriormente se procedió a la siguiente etapa, consistente en la aplicación de los instrumentos para la recopilación de la información, con ello se realizó una evaluación de la micro y pequeña empresa de El Salvador, con el fin de conocer el estado actual de dichas empresas y evaluar la aplicabilidad de buenas prácticas seleccionadas a ellas. Como etapa final se elaborará un manual de buenas prácticas aplicables a la micro y pequeña empresa de El Salvador, así como una matriz de costo.

En el primer capítulo, se enuncia la problemática que enfrentan las micro y pequeña empresa con la administración de las diferentes TIC que tienen, desde un celular para hacer negocios a través de las redes sociales hasta una computadora ejecutando una aplicación para control administrativo de las operaciones del negocio. Así mismo, se plantean las metodologías más robustas que apoyan la administración, buena gestión y seguridad de la información que cada empresa genera día tras día.

En el segundo capítulo, se describe cada una de las partes fundamentales que componen las metodologías de ITIL, COBIT y seguridad de la información basados en la norma ISO 27001.

Es muy importante conocer a profundidad el contenido de cada una para determinar cuáles son aquellas prácticas sugeridas que aportan un valor agregado a la gestión de las TIC de las empresas; lo objetivo es evaluar cada una, identificando su criticidad, importancia y esfuerzo requerido, determinando si encaja o no en la capacidad que las micro y pequeñas tienen.

En el tercer capítulo, se detallan las unidades de análisis en las que se divide el trabajo de graduación, estas son las partes que se han considerados importantes y básicas que una empresa debe controlar. De esto se determinan las diferentes variables que nos permiten evaluar cada herramienta y las prácticas orientadas a cada unidad de análisis.

En el cuarto capítulo, se expresan los resultados obtenidos, a partir de la aplicación de las técnicas e instrumentos definidos en el capítulo tres. Dando respuesta a cada variable especificada por cada unidad de análisis.

En el quinto capítulo se describe el proceso de construcción de la guía de buenas prácticas, desarrollada a partir de los resultados obtenidos en el capítulo cuatro.

El sexto capítulo expresa las conclusiones y recomendaciones consensuadas a partir de la problemática, revisión del estado del arte y resultados obtenidos a partir de la metodología descrita.

1. Capítulo I. Planteamiento del problema

1.1. Descripción del problema

Actualmente en El Salvador, las TIC se han convertido en una herramienta estratégica para el crecimiento económico y social del país, todas estas aplicadas en las diferentes empresas que conforman el motor que mueve la economía. Sin embargo, aún hay sectores comerciales que cuentan con tecnologías básicas (Computadora y ofimática; o en el peor de los casos no se tiene ninguna) para el manejo de sus negocios, tal es el caso de las micro y pequeñas empresas, que carecen de una orientación o una visión de cómo las tecnologías pueden impulsar al crecimiento y migrar a un mayor nivel. Ejemplo de ello, un análisis realizado en el sector educativo enmarca el potencial de las buenas prácticas de tecnología de información como impulsores de la competitividad y el desarrollo social, encaminándolos a la actualización continua y extendiendo el aprendizaje mediante educación a distancia (1 pág. 181).

Existen muchas limitantes que pueden inferir en la implementación de buenas prácticas en las micro y pequeña empresa, principalmente si se centra en el tamaño, de las cuales y de manera hipotética se deduce que no se cuenta con el personal necesario para llevar a cabo dichas mejoras. Pero, no solo se trata de recursos humanos, también hay factores que influyen tales como los planteados en el artículo “Problemas en la adopción de modelos de gestión de servicios de tecnologías de información” (2), lo cual puede inclinar el camino a seguir y que las empresas desistan de la aplicación de actividades encaminadas a convertir las TIC en un eje transversal estratégico de sus negocios.

Los lineamientos contenidos en ITIL, COBIT 5, y la gestión del riesgo (Norma ISO-27001), se alinean a los objetivos del negocio orientándose a resultados, dando la mayor seguridad que no se está gastando dinero ni tiempo, ya que cada elemento tecnológico administrado, creado o adquirido está fundamentado por las necesidades propias del negocio. Lastimosamente, estas metodologías requieren de presupuesto, esfuerzo y personas que lo lleven a cabo, esto debido a todas las capas integradas y criterios de aplicación; sin embargo, hay recomendaciones vitales que se pueden extraer para ser aplicados en ambientes donde las TIC están dando sus primeros pasos o ya están caminando, pero necesitan ser administrados.

Con este trabajo de graduación, se elaborará un modelo que recopile buenas prácticas de cada metodología y que se pueda implementar en la micro y pequeña empresa en El Salvador, llevándolas a estar preparadas cuando migren a un nuevo nivel de categoría como mediana empresa.

1.2. Antecedentes

En El Salvador, desde la publicación del Libro Blanco de la Microempresa en 1996, el tema de la micro y pequeña empresa ha sido una de las principales preocupaciones de los diferentes sectores y gobiernos, y es el resultado de una investigación sobre el desempeño de las microempresas y su trascendencia en la vida económica y social de la nación.

De igual forma, el Programa de Desarrollo de la Microempresa (FOMMI II) difundió, junto con el Ministerio de Economía (MINEC) por medio de la Dirección General de Estadísticas y Censos (DIGESTYC) en 1999, una encuesta sobre la Microempresa con el propósito de sustentar los aspectos de las estrategias de política y de apoyo a la microempresa salvadoreña. El mayor esfuerzo del Ministerio de Economía en conjunto con la Comisión Nacional de la Micro y Pequeña Empresa (CONAMYPE) se realizó en el año 2001, cuando se publicó el informe "Características del Sector de la Microempresa Salvadoreña-1999 (3), donde se analizó el estado de la situación de la microempresa salvadoreña y se agregaron datos sobre el entorno económico de la economía salvadoreña.

Posteriormente, en 2005, el Ministerio de Economía publica el estudio "Dinámica de MYPE en El Salvador": Este estudio, realizado por la DIGESTYC con la coordinación general de CONAMYPE, se llevó a cabo entre noviembre de 2003 y abril de 2004 (3), con el fin de brindar información anual sobre el desempeño del sector. En el informe se incluyó un análisis y descripciones, tanto de la micro, como de la pequeña y mediana empresa, y de acuerdo con la definición que conceptualmente concibió la propia CONAMYPE. Además, se introdujeron elementos para la evaluación de su dinámica, rescatándose puntos importantes sobre el estado de estas empresas, además de permitir tener una estimación de la cantidad de MYPE en el país.

Enlazado con investigaciones anteriores, en 2017 a través de la unificación de esfuerzos entre CONAMYPE, DIGESTYC y el BCR, los ciudadanos son informados sobre la "Encuesta Nacional de Micro y Pequeñas Empresas 2017", un documento en el que se define el estado actual de MYPE. Este estudio se llevó a cabo a nivel nacional, con la representación a nivel urbano y rural, por departamento y región.

Según la metodología utilizada para dicha encuesta, se definieron una muestra de 829 segmentos a ser censados de la DIGESTYC, los cuales se agruparon en urbanos y rurales.

“Definiendo, al interior de estos, los tipos de estructuras que habría de considerar fueran negocios y viviendas únicamente, para posteriormente realizar una distribución de estos por zona geográfica de manera aleatoria, siendo el objeto de la investigación” (3).

1.3. Objetivos

1.3.1. Objetivo general

Elaborar un modelo de buenas prácticas de TIC en la micro y pequeña empresa en El Salvador.

1.3.2. Objetivos específicos

- Analizar cada una de las partes integradas por las metodologías de TIC más reconocidas.
- Evaluar cada metodología basada en la dimensión del sector micro y pequeña empresa en El Salvador.
- Consolidar las buenas prácticas de TIC aplicables a la micro y pequeña empresa en El Salvador.

1.4. Justificación

Las MYPE son un factor esencial de la economía de El Salvador, conformadas por un total de 317,795 establecimientos (3), y no son ajenas a la utilización de TIC. No tener un modelo o método de cómo administrar los recursos tecnológicos, o incluso obtener el mejor potencial de estos, puede llevar a este sector económico a sufrir condiciones que transgredan su crecimiento. El avance constante y el surgimiento de nuevas plataformas tecnológicas sugieren un mayor énfasis en su control y mantenerlas alineadas a los objetivos del negocio, pero ¿Por qué?, esto se debe a dos factores importantes que se deben cuidar: finanzas e información de la empresa.

Las TIC permiten a las empresas apoyar sus negocios en el potencial que ofrecen, teniendo de la mano el control de estas, basándose en las buenas prácticas que contienen. Dicho esto, las MYPE tienen amplias oportunidades de crecimiento a través del uso de la tecnología, el cual es la finalidad de este trabajo de graduación, el crear un modelo de buenas prácticas recopiladas de las metodologías más reconocidas para la administración de servicios TIC y que estén enfocadas a los objetivos estratégicos de ellas, velando por los factores importantes que se deben cuidar mencionados anteriormente.

1.5. Delimitación

1.5.1. Alcances

- Se creará un modelo de buenas prácticas recopiladas de las metodologías ITIL, COBIT y norma ISO 27000.
- Se identificarán los lineamientos básicos definidos en la norma y las metodologías seleccionadas.
- El sector económico al que aplica este trabajo de graduación es a las MYPE de El Salvador.
- El trabajo de graduación solo llegará a realizar el modelo de buenas prácticas para MYPE en El Salvador.
- Únicamente se realizará un documento con los lineamientos que acoplen a las MYPE de El Salvador.

1.5.2. Limitaciones

- Las condiciones propias de las MYPE en El Salvador en cuanto a temas financieros y de personal.
- Únicamente se utilizarán las metodologías ITIL y COBIT 5 por ser modelos de gestión de servicios TIC y la norma ISO 27001 por su orientación a la seguridad de la información.

2. Capítulo II. Estado del arte

2.1. Definición y características de las micro y pequeña empresa

Según la ley de fomento, protección y desarrollo para la micro y pequeña empresa (4)

Microempresa: persona natural o jurídica que opera en los diversos sectores de la economía, a través de una unidad económica con un nivel de ventas brutas anuales hasta 482 salarios mínimos mensuales de mayor cuantía y hasta 10 trabajadores.

Pequeña empresa: persona natural o jurídica que opera en los diversos sectores de la economía, a través de una unidad económica con un nivel de ventas brutas anuales mayores a 482 y hasta 4,817 salarios mínimos mensuales de mayor cuantía y con un máximo de 50 trabajadores.

Cuando una persona natural o jurídica no reúna las condiciones previamente establecidas, su clasificación se determinará por sus ventas brutas anuales. Las entidades públicas y privadas deberán uniformar las características antes definidas y los criterios de medición, a fin de construir una base de datos homogénea que permita dar coherencia al diseño y aplicación de las políticas públicas de promoción y formalización del sector.

En El Salvador existe un ente gubernamental el cual se encarga de velar por los intereses de dichas empresas, llamado “Comisión Nacional de la Micro y Pequeña Empresa” CONAMYPE.

Según CONAMYPE, las Micro y Pequeñas Empresas MYPE representa cerca del 99% (5) del sector empresarial del país; además se estima que estas empresas generan alrededor de 700 mil empleos directos y aportan aproximadamente el 35% del Producto Interno Bruto PIB.

En el ámbito tecnológico las MYPE no han incursionado debido a la inversión que se requiere y que muchas a lo mejor logran un ingreso igual a de un salario mínimo (6). Las empresas de menor tamaño y en especial las microempresas enfrentan importantes dificultades para la adopción de tecnologías de información y comunicación TIC.

Uno de los aspectos principales que han hecho que las MYPE no adopten el uso de TIC, es el acceso a banda ancha, ya que es fundamental para que las empresas puedan realizar transacciones electrónicas y aprovechar plenamente las posibilidades de Internet. Sin embargo, el precio de la banda ancha fija sigue teniendo costos elevados (7).

Las TIC son piezas fundamentales en el actual mundo económico y empresarial. Su implantación en la empresa permite la modernización y agilización de los procesos, incrementar los niveles de productividad, innovar y, en definitiva, aumentar la competitividad de la empresa en un mercado competitivo.

La digitalización de las empresas es un proceso complejo y progresivo que está directamente relacionado con la evolución de la organización del negocio.

Algunos factores por los que las MYPE se ven beneficiados por las TIC son:

- 1) Permiten tener información rápida y eficaz para la toma de decisiones.
- 2) Reducen los costos de las transacciones (con clientes y proveedores).
- 3) Permiten automatizar los procesos internos para volverse más eficiente.
- 4) Facilitan los procesos de aprendizaje en su equipo humano.

Actualmente existe una estrategia en el país a fin de lograr la inclusión de las MYPE a las TIC, dicha estrategia está conformada por 4 líneas de acción (4) que son:

Línea 1: mejora del entorno para el acceso y accesibilidad.

Este punto tiene como objetivo fomentar el uso cotidiano de las TIC en diferentes áreas del negocio para obtener, procesar y generar información de valor para la toma de decisiones (7). Para ello se crearán centros digitales para el aprendizaje de las TIC y se crearán planes de financiamiento para equipar a las MYPE con equipo tecnológico.

Línea 2: desarrollo de habilidades digitales.

Se tiene como objetivo el desarrollo de habilidades digitales en personas empresariales y trabajadores de las MYPE. Para ello se promoverán la alfabetización digital de personas emprendedores y empresarias en todo el país; además la creación de recursos electrónicos que permitan la formación sobre el uso de herramientas TIC en las empresas.

Línea 3: innovación y crecimiento industrial TIC nacional

El objetivo de este punto es el de contribuir al fortalecimiento empresarial de la industria TIC nacional con el propósito de que los productos o servicios respondan a las necesidades de las MYPE salvadoreñas. Para ello se brindarán los espacios físicos y virtuales necesarios a fin de que se logren identificar las necesidades de dichas empresas y brindar propuestas de solución a las mismas; además de promover emprendimientos relacionados con las TIC.

Línea 4: desarrollo de una cultura de uso de las TIC en la MYPE

Este punto tiene como objetivo fomentar una nueva cultura en torno al uso de las TIC para lograr mejores niveles de productividad y competitividad. Para ello se pondrá en funcionamiento un sistema de información web sobre los servicios TIC para los emprendedores y empresarios; además se crearán campañas para difundir la importancia de las TIC para el crecimiento de dichos negocios.

2.2. COBIT

2.2.1. ¿Qué es?

COBIT, en su versión 5, es un marco de referencia de gobierno de TI y un conjunto de herramientas de soporte, la cual permiten a gerentes disminuir la brecha entre los requerimientos de control, los temas técnicos y riesgos de negocio. Además, permite el desarrollo de una política clara y buena práctica para el control de TI en las organizaciones. Dicho marco de trabajo acentúa el cumplimiento regulatorio, ayuda a las organizaciones a incrementar el valor asociado el área de TI, habilita la alineación y simplifica la puesta en práctica del marco de referencia (8). COBIT ha venido evolucionando a lo largo del tiempo tal y como se muestra en la siguiente figura 1:

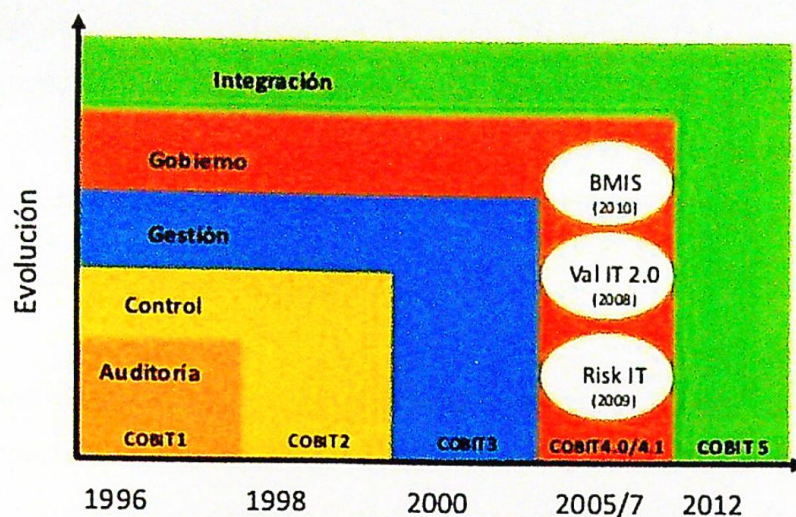


Figura 1: evolución de COBIT.

Obtenido de: Introducción a COBIT 5 (9)

COBIT es como un mapa que brinda una guía completa de qué deben tener en cuenta dentro de los departamentos de TI de las empresas para garantizar que las operaciones del negocio se puedan llevar a cabo. No se trata solamente de gestionar la seguridad, de tener aplicaciones, procesos o servidores. Es ir un paso más adelante, es la implementación de un proyecto que permite a cualquier organización integrar toda su gestión de TI y que debería velar por alinearla con la operación del negocio (10).

COBIT surge con la misión de investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información para ser utilizados diariamente por gerentes de negocio y auditores. COBIT 5 posibilita que TI sea gobernada y gestionada en forma integral para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos.

COBIT es empleado en todo el mundo por quienes tienen como responsabilidad principal los procesos de negocio y la tecnología, aquellos de quien depende la tecnología y la información confiable, y los que proveen calidad, confiabilidad y control de TI. Este marco de trabajo se basa en el gobierno de TI y el gobierno Corporativo.

El gobierno corporativo se define como el conjunto de responsabilidades y practicas ejecutadas por la junta directiva y la alta gerencia con el fin de brindar la dirección estratégica

del negocio. En cambio, el gobierno de TI según Macgregor (11), es una estructura de relaciones y procesos para dirigir y controlar la empresa con la finalidad de lograr los objetivos corporativos mediante la adición de valor, mientras simultáneamente se encuentra el equilibrio entre el riesgo y el retorno sobre las inversiones en TI y sus procesos.

2.2.2. Características.

COBIT provee un marco global que permite a las empresas a alcanzar sus objetivos para el gobierno y la gestión de TI, es decir, ayuda a las empresas a crear valor manteniendo equilibrio entre los beneficios obtenidos, la optimización de los niveles de riesgo y el uso de los recursos.

COBIT permite gobernar y gestionar de manera integral toda la empresa desde la perspectiva de TI, cubriendo todo el negocio, las funciones y responsabilidades de TI, teniendo en cuenta permanentemente los intereses relacionados con TI.

Enfoque hacia procesos, mediante un modelo que subdivide TI en 34 procesos de acuerdo con cuatro áreas de responsabilidad (Planear, Construir, Ejecutar y Monitorizar) que básicamente coinciden con el conocido ciclo de Deming.

COBIT presenta una dualidad de orientación hacia el Negocio y hacia las TIC, estableciendo un puente de enlace entre ambos mundos y definiendo un lenguaje común que ha permitido a la gerencia entender el valor estratégico de las TIC y a los responsables de los sistemas de la información, la importancia de conducir sus acciones hacia el aporte del valor al negocio.

2.2.3. Principios.

COBIT 5 se basa en 5 principios, detallados en la figura 2:

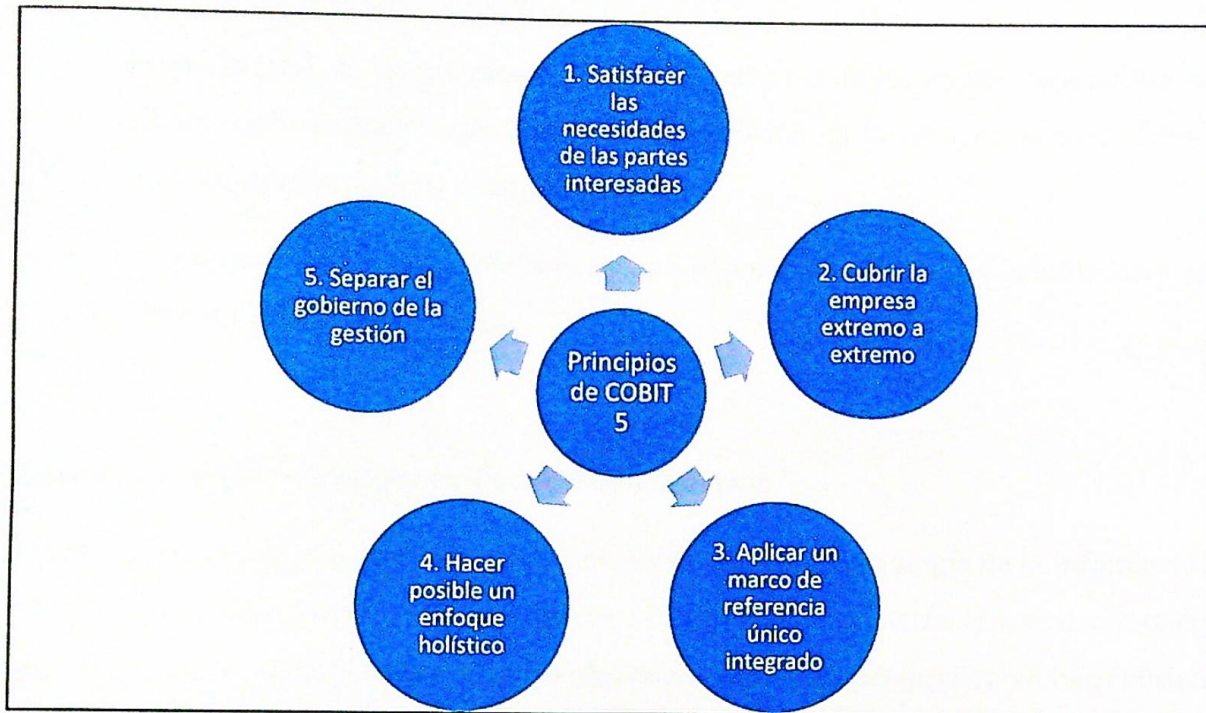


Figura 2: Principios de COBIT 5.

Elaboración propia, fuente ISACA.

Principio 1: Satisfacer las necesidades de los interesados

Este principio busca que todas las partes interesadas alinear todos sus objetivos y recursos con los de negocio, mediante el uso de la negociación. El gobierno de TI deberá considerar a todas las partes interesadas al tomar decisiones con respecto a la evaluación de riesgos, los beneficios y el manejo de recursos.

Las necesidades de las partes interesadas deben ser transformadas en una estrategia para la organización. COBIT hace uso de las metas en cascada, la cual transforma las necesidades de las partes interesadas en metas específicas que pueden realizarse.

Uno de los beneficios de las metas en cascada de COBIT, es definir las prioridades para implementar, mejorar y asegurar el gobierno corporativo de la TI, en base de los objetivos de la organización y los riesgos relacionados:

En la práctica, las metas en cascada:

- Definen los objetivos y las metas tangibles y relevantes, en diferentes niveles de responsabilidad.
- Filtran la base de conocimiento de COBIT, en base de las metas corporativas para extraer una orientación relevante para la inclusión en los proyectos específicos de implementación, mejora o aseguramiento.
- Claramente identifican y comunican qué importancia tienen los habilitadores para lograr las metas corporativas.

Principio 2: Cubrir la empresa de extremo a extremo

COBIT se concentra en el gobierno y la administración de la tecnología de la información y relacionadas desde una perspectiva integral a nivel de toda la organización, es decir, tanto el gobierno de TI, como la gestión de TI son abordados desde una perspectiva global, cubriendo todas las necesidades corporativas de TI.

Principio 3: Aplicar un único marco de referencia integrado

COBIT integra los mejores marcos de ISACA como Val IT, Risk IT, etc. Además, permite alinearse con los principales estándares o marcos como Information Technology Infrastructure Library (ITIL®), Project Management Body of Knowledge (PMBOK), Committee of Sponsoring Organizations of the Treadway Commission (COSO) y estándares ISO, entre otros.

Principio 4: Posibilitar un enfoque holístico

COBIT identifica los habilitadores clasificados en 7 categorías que abarcan la empresa en su totalidad, estos son factores que individual y colectivamente influyen para que el gobierno y la gestión de TI operen de acuerdo con las necesidades del negocio.

Principio 5: Separar el gobierno de la gestión

COBIT distingue claramente entre gobierno de TI y la gestión de TI. Por un lado, el gobierno asegura que los objetivos empresariales se logren evaluando las necesidades de todos los interesados del negocio. En cambio, la gestión, se ocupa de planificar, construir, ejecutar y monitorear las actividades alineadas con la dirección establecida por el organismo de gobierno para el logro de los objetivos empresariales.

2.2.4. Procesos.

COBIT en su versión 5 posee 37 procesos, divididos en 5 dominios, detallados en la figura 3:

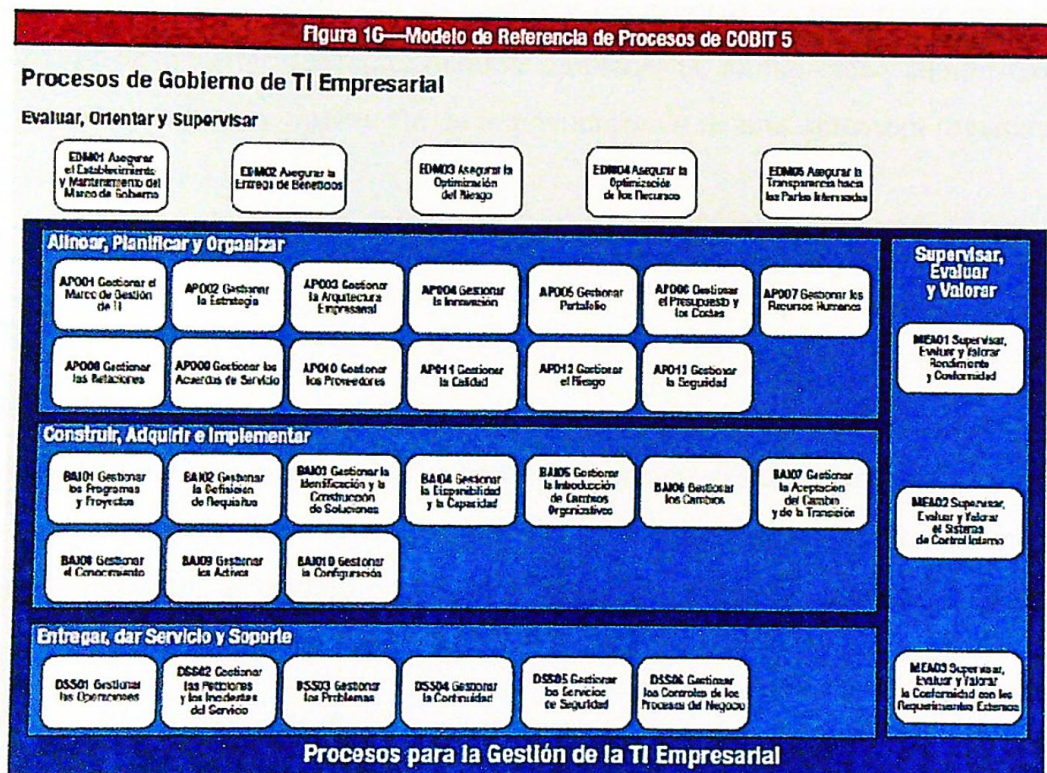


Figura 3: dominios y procesos de COBIT

Fuente ISACA.

Dominio 1: evaluar, orientar y supervisar

La evaluación, orientación y supervisión es parte de la responsabilidad de los gerentes de la compañía quienes son los invitados a tomar acciones sobre este dominio perteneciente al Gobierno de IT y que cuenta con cinco procesos, mediante los cuales se encarga de asegurar el establecimiento y mantenimiento de un marco de gobernanza, haciendo que los beneficios se concreten, a través de la optimización de riesgos y recursos manteniendo la transparencia hacia los interesados, es decir hacia la alta gerencia de la compañía (12).

Dominio 2: alinear, planear y organizar

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir mejor con los objetivos del negocio. Es importante mencionar que la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas; y finalmente, la implementación de una estructura organizacional y tecnológica apropiada (13).

Este dominio proporciona la dirección para la entrega de soluciones y la entrega de servicios.

Dominio 3: construir, adquirir e implementar

Este dominio representado por 10 procesos es el encargado de diseñar e implementar las soluciones que indique el dominio 2, con un enfoque en gestionar programas y proyectos, definir los requisitos, identificar y construir soluciones, gestionar la disponibilidad y capacidad, introducir el cambio organizativo, gestionar cambios, aceptar los cambios y la transición, gestionar también el conocimiento, los activos y la configuración.

En este dominio se planean todos los procesos que se planearon en el dominio anterior. En esta fase ya estamos trabando en un servicio que vamos a implementar en la organización, aquí se construye el servicio, lo lleva a prueba, se hace toda la documentación.

Dominio 4: entregar, dar servicio y soporte

Involucra la entrega en sí de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte a los usuarios del servicio, la administración de los datos y de las instalaciones operativas.

El objetivo es lograr que los servicios de TI se entreguen de acuerdo con las prioridades del negocio, la optimización de costos, asegurar que la fuerza de trabajo utilice los sistemas de modo productivo y seguro, implantar de forma correcta la confidencialidad, la integridad y la disponibilidad.

Dominio 5: supervisar, evaluar y valorar

Dentro de este dominio, se encuentran 3 procesos que se encargan del rendimiento y conformidad, el sistema de control interno y la conformidad con los requerimientos externos, los mismos que son vitales en el giro del negocio de la compañía, debido a que por medio de las mediciones y el control permanente se garantiza la eficiencia operativa y permite encontrar oportunidades de mejora a los procesos que maneja el área de TI.

2.3. ITIL

2.3.1. ¿Qué es?

Information Technology Infrastructure Library (ITIL), es un marco de trabajo con buenas prácticas orientadas a la administración de servicios de TIC, habilitando la documentación de procesos informáticos y de comunicaciones garantizando que los proveedores y clientes de estos servicios estén alineados a los objetivos del negocio. ITIL orienta sus esfuerzos principalmente en la gestión del servicio, fortaleciendo su definición y orientación al negocio, es decir, que este aporte un valor real a las operaciones.

Entonces, según ITIL ¿Qué es un servicio? Es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad que estos asuman los costes y riesgos específicos asociados (14).

La gestión de los servicios, tanto interno como externos, es un tema que en muchas empresas no se aborda, o solamente se tiene una concepción o percepción de “buen servicio”. Esto no trata únicamente de una evaluación en base a 5 estrellas (siendo perfecto), o un buen porcentaje de retroalimentación; el objetivo principal de la gestión de los servicios es que estos realmente aporten un beneficio a los negocios de la compañía, los cuales en conjunto sean competitivos, abriendo posibilidades de cerrar nuevos negocios y fidelizar clientes (15).

Cada servicio trae consigo un esfuerzo que el negocio debe realizar, que al final se traduce en dinero. Para un negocio las inversiones se basan en objetivos que a corto o largo plazo

retornen un beneficio alto (sobrepasando lo invertido), difícilmente se hacen negocios pensando en perder, realmente se pierde cuando estos se realizan con poco o nulo conocimiento de la verdadera necesidad, sus alcances, limitaciones y si hay posibilidad de mejorar lo que actualmente se tiene. Por ejemplo, algo muy común es el problema que se tiene con el ancho de banda de internet, que al no estar bien administrado tiende a comportarse de manera irregular; normalmente lo que se concluye de primera mano es que el ancho de banda es demasiado ajustado y que lo mejor es aumentarlo (He aquí el tema inversión). ¿Qué es lo más acertado en una situación como esta? Determinar las causas y posibles soluciones, tomando en consideración si se pueden reutilizar los elementos con los que se cuenta, o en un determinado caso, la planificación de los cambios necesarios para mejorar el servicio.

Para lo anterior, es necesario identificar los diferentes servicios que se tienen, al menos en algún listado, y como primer punto tratar de clasificarlos. Estos se pueden clasificar de las siguientes maneras:

- Servicios locales, son aquellos que se proveen de manera autónoma para satisfacer una necesidad específica del negocio, por ejemplo, limpieza, vigilancia, albañilería, tapicería, plomería, mantenimiento general de equipos, informática, etc. Estos pueden estar relacionados con los procesos de negocio principales o ser indistintos a estos.
- Servicios externos, se refiere a aquellos que se obtiene de proveedores y que tienen una relación directa o indirecta con los procesos de negocio a los que se dedica la empresa.

Es muy importante esta clasificación debido a que puede cambiar el rumbo de las decisiones que se estén tomando y que están próximas a tomarse. Es normal que todos los servicios que requiere un negocio para mantenerlo en marcha se lleven de manera local (autónoma), implicando el manejo de la totalidad de los costos, esfuerzos y riesgos que estos traen consigo. Pero, hay una alta probabilidad que muchos de estos no estén relacionados con los servicios propiamente del negocio. Por ejemplo, un restaurante puede optar por contratar de manera interna un carpintero para que le de mantenimiento a la mueblería del lugar, encargándose de todo lo que esto implica: compra de herramientas, materiales, personal, pagos de fondo de pensión, seguro social, etc., pero también puede optar por subcontratar

dicho servicio y establecer un contrato con un proveedor que supla las necesidades, permitiendo invertir más en aquellos procesos que están directamente relacionados con los servicios ofertados.

2.3.2. Descripción de las fases del marco de trabajo

La gestión de los servicios a través de ITIL se divide en 5 fases que son:

- a. Estrategia del servicio
- b. Diseño del servicio
- c. Transición del servicio
- d. Operación del servicio
- e. Mejora continua

Cada una de ellas incluye una serie de prácticas que definen y controlan el servicio partiendo desde el momento en que un servicio es solicitado hasta que este es puesto en marcha. La documentación generada y los resultados obtenidos de cada fase sirven de insumo para la que precede, esto con la finalidad de apoyar las decisiones y prácticas que requieren de información generada previamente y que debe de contar con información específica del negocio y el servicio.

A medida se adentra al estudio de las fases, es evidente que la base fundamental de ITIL es la documentación, la cual sigue siendo un punto débil de muchos negocios emergentes, y es aquí donde surge la pregunta ¿Es posible que negocios se pierdan por falta de información o por no tener claridad de cara al negocio? Se podría contestar con otra interrogante ¿se podrá cerrar un negocio importante suponiendo que se tiene lo que se negocia?

La información que cada micro y pequeña genera puede servir de punta de lanza para identificar oportunidades de negocio, búsqueda de innovación y encaminarse a un crecimiento financiero que habilite la diversificación y mejora continua de los procesos de negocio. Muchos negocios en El Salvador partieron de prácticas empíricas y en ocasiones heredadas por generaciones, pero ocuparon todas sus fuentes de información para solidificar sus procesos y que, gracias a ello, han logrado posicionarse en el mercado a lo largo de los años. No todo negocio inicia con un fuerte capital, inversionistas interesados y tecnológicamente respaldados, muchos iniciaron con un cuaderno o una lista de ventas

haciendo sumas y restas al final de cada jornada cuadrando ventas, contando inventario, etc., ahora se han convertido en empresas solidas con un amplio margen de inversión en la diversificación de sus productos y sus procesos.

ITIL sustenta cada fase con documentación para dar claridad de los servicios que se requieren, permitiendo la facilidad de toma de decisiones a través de la claridad del objetivo de cada servicio y lo que implica cada uno de estos. No se trata de habilitar servicios solo porque es una moda o un modelo mundialmente utilizado, se trata de que dicho servicio realmente aporte valor al negocio y que lo vuelva más competitivo. Esto permite que se implemente aquello que realmente es funcional y a un costo equilibrado con la capacidad que se tiene.

Cuantas empresas realizan inversiones tecnológicas por servicios que, sin una base documental, terminan convirtiéndose en un gasto que puede poner en peligro su crecimiento disminuyendo su capacidad de inversión. ITIL, trata de fundamentar dichas inversiones a través de documentos que sustenten las condiciones de cada servicio, como opera, como se distribuye, las capacidades instaladas, acuerdos de servicio, contratos, garantías, etc., todo con el objetivo de respaldar al negocio y que tenga una visión clara de las condiciones e indicadores establecidos para asegurar que se está llevando el rumbo correcto.

Iniciar con ITIL para las micro y pequeñas empresas, supone un esfuerzo que los supera en personal necesario y recursos financieros, pero se puede iniciar con prácticas que apoyen a definir la capacidad, continuidad y disponibilidad de los servicios, acompañados con mejoras que permitan administrar los problemas relacionados a los productos de TI y que amenazan las operaciones del negocio (16). Este inicio da paso a una generación de conocimiento que apoya a la toma de decisiones, y es que, los resultados obtenidos en su aplicación permiten que la información se centralice y esté disponible para la generación de informes, o análisis inmediatos que se requieran, todo esto con la certeza de cómo funcionan los procesos de negocio y las capacidades con las que se cuentan para llevar a cabo nuevos negocios, o por otra parte, si los objetivos de negocio se están cumpliendo (17).

2.3.3. Estrategia del servicio

Todo servicio TIC que se tenga dentro de una empresa debe estar alineada al negocio, esto tiene un alto impacto en el cumplimiento de los objetivos establecidos y que la mantenga en un nivel competitivo.

Como punto de partida es necesario establecer los servicios a brindar y como estos se llevarán a cabo, luego definir el valor que aporta al negocio, identificación de clientes, entre otros (14).

ITIL orienta los servicios hacia la creación de valor, ya que deben de cumplir un objetivo de negocio específico que garantice que la relación entre cliente-negocio se mantenga en ganar-ganar, de igual forma cuando se trata de contratar un servicio a un proveedor. El aumento de la competitividad se asocia al aumento de ventas y negocios ejecutados, pero no se puede desacreditar que las TIC son una base fundamental para que estos factores de éxito se materialicen (18).

Otro concepto importante que forma parte de la estrategia de un servicio es la utilidad, la cual debe cumplir con lo que se requiere, aumente el rendimiento y que represente una disminución de costos, o de lo contrario, aumento en los ingresos.

A la par de la utilidad, pero no menos importante, se tiene el termino garantía, el cual da la seguridad al cliente y al negocio de la disponibilidad que tiene de usarla, cuáles son las condiciones que la vuelven efectiva y respaldo de continuidad ante cualquier situación que se presente. Tanto la garantía como la utilidad van de la mano y mantienen un equilibrio garantizando una buena percepción que el servicio es el ideal.

La estrategia del servicio se apoya de los elementos siguientes:

- Gestión financiera
- Gestión del portafolio de servicios
- Gestión de la demanda

2.3.4. Diseño del servicio

Esta fase de encarga de diseñar nuevos servicios o modificar los ya existentes, procurando su alineación con las necesidades de los clientes, con rentabilidad, cumpliendo estándares de calidad y como punto principal el aporte de valor a los clientes (14).

Diseñar no solo implica la ejecución de integración de componentes al servicio, también lleva consigo consideraciones sobre los requisitos y los recursos con los que se cuentan para cumplirlos. La estrategia del servicio se encargó, en primera instancia, de definir las reglas del juego y las especificaciones propias del servicio que deben cumplirse y mantenerse hasta las etapas finales del servicio en ejecución.

ITIL sugiere una serie de principios de diseño del servicio que son:

- Diseño de soluciones del servicio
- Diseño del portafolio de servicios
- Diseño de la arquitectura del servicio
- Diseño de procesos
- Diseño de métricas

ITIL también sugiere tres modelos de diseño con los cuales se puede trabajar un servicio, estos son:

- Modelo tradicional
- Modelo ágil
- Soluciones empaquetadas

El uso de estos modelos dependerá del o los objetivos que debe cumplir dicho servicio. Por ejemplo, una empresa que ofrece software modular puede optar por un modelo ágil que le permita poner en marcha el sistema añadiendo características nuevas cada vez que se finalice la etapa de desarrollo. Esto no solo integra sistemas desarrollados internamente, también puede ser aplicados con proveedores a través de los acuerdos que se tomen.

Los procesos que la fase de diseño integra son los siguientes:

- Gestión del catálogo de servicios
- Gestión de niveles de servicio

- Gestión de la capacidad
- Gestión de la disponibilidad
- Gestión de la continuidad de los servicios de TI
- Gestión de la seguridad de la información
- Gestión de proveedores

El diseño del servicio define el cómo se aplicará la estrategia para la que está orientado el servicio, aquí es donde se cimentan las bases en las que el servicio se apoyara para cumplir con sus objetivos (19). Algo muy importante que se identifica en esta fase es que no solo se trata de desarrollo, o un término más genérico, “*carpintería*”, se enfoca también en la documentación, dejando clara las especificaciones del servicio, sus condiciones de funcionamiento y niveles de seguridad que han sido contempladas para su operación.

2.3.5. Transición del servicio

Uno de los elementos principales que acompaña a un servicio determinado, es su despliegue. Se debe garantizar principalmente que su transición de la etapa de diseño a producción sea exitosa, ¿Quién arriesgaría operaciones importantes de negocio por un despliegue de servicios sin garantías? Lo importante, y se puede colocar como el objetivo estratégico de esta fase, es poner a disposición del cliente el servicio y que este cuente con todas las especificaciones solicitadas.

La experiencia de transición de servicios de cara al cliente debe suponer una manera donde el cliente sienta la seguridad y que cuente finalmente con lo que ha solicitado. Por eso, esta fase toma en consideración todos los elementos establecidos en las fases de estrategia y diseño, ahí se encuentran cimentadas las necesidades, configuraciones y especificaciones propias del nuevo servicio. Por ende, se debe de asegurar que en esta etapa se integren cada uno de esos detalles, esto mejora la experiencia del cliente y la capacidad de los controles establecidos por la parte encargada de aplicar esta fase, todo esto orientadas a minimizar riesgos que pueda estar implicados en esta etapa.

La transición inicia con un primer precedente que pone en perspectiva la necesidad de modificar o crear un servicio, este es el RFC (Request For Change) (14). Normalmente, en

las TIC, siempre existe una necesidad o una dificultad que da paso a la generación de una RFC, estos habilitadores pueden ser:

- Agregar un servicio nuevo
- Modificar un servicio existente
- Un error que habilite cualquiera de las anteriores
- Actualizar un software de tercero
- Cambios de carácter legal

Esto permite, a la fase de transición, tener una perspectiva general del servicio que se está tratando, no es lo mismo poner en operación una solicitud de reporte, que una modificación asociada a las facturaciones de un negocio. Por ello esta fase define tres procesos que se describen de la siguiente manera:

- **Estrategia:** Encargada de definir lo necesario para llevar a cabo las operaciones necesarias para la puesta en producción del servicio, incluyendo partes interesadas, aspectos externos (legales, institucionales, proveedores, etc.), roles, entre otras.
- **Preparación:** Se encarga de revisar que se cuente con toda la información necesaria para llevar a cabo la transición, garantizando que toda la información está debidamente actualizada y disponible.
- **Planificación:** Detalla el flujo de trabajo bajo el cual se hará la transición, esto incluye las actividades antes, durante y después de la transición, posterior a los resultados de evaluación post-transición determinar el cierre de la transición.

Los procesos que acompañan a la fase de transición de servicios son:

- Planificación y soporte a la transición
- Gestión de cambios
- Gestión de la configuración y activos del servicio
- Gestión de entregas y despliegues
- Validación y pruebas
- Evaluación
- Gestión del conocimiento

Es muy importante tomar en cuenta que esta etapa debe considerar la actualización a manuales de configuración, de usuario, de sistema, etc., según lo que se requiera para que el nuevo servicio implementado cuente con la documentación necesaria, esto permitirá que cualquier parte interesada pueda consultarlos y tener la claridad del objetivo del servicio y de todas las características con las que opera, tanto sus dependencias como sus resultados esperados.

2.3.6. Operación del servicio

Esta fase, definida como crítica (14), se encarga de controlar que el servicio cuente con las configuraciones necesarias para su correcta operación y que cumpla con los objetivos. La definición crítica tiene relación con todo comportamiento que puede impactar negativamente las operaciones del negocio, por ello esta fase es muy importante y crucial, ya que la información generada es un insumo directo para la fase de mejora continua.

Una actividad intrínseca dentro de esta fase es el soporte al cliente, una actividad que, aunque puede parecer sencilla, influye directamente en el éxito del servicio. Se trata, principalmente, de lograr estabilidad en el servicio, y que el cliente tenga de conocimiento la disponibilidad del servicio. Ante esto, es importante que se cuente con una actitud proactiva (14), es decir, la capacidad de atender anticipadamente cualquier comportamiento del servicio y evitar que esto se vuelva una urgencia. Sucede en muchas ocasiones que la falta de proactividad por parte de los encargados de las TIC genere una serie de dudas sobre el servicio y sus resultados, dado que los clientes son los primeros en recibir el impacto de un comportamiento aleatorio diferente a lo establecido.

Dada la necesidad de proactividad para la determinación de cualquier eventualidad no contemplada, se puede decir que no se deben admitir sorpresas, ya sean buenas o malas, una sorpresa es un lujo que no se puede dar en las TIC, todo debe estar debidamente controlado y acorde a los niveles de calidad y resultados acordados.

Los riesgos inherentes en los servicios implementados deben identificarse previamente, de ser posible desde la estrategia del servicio, tomando en cuenta los elementos de configuración e infraestructura sobre la que opera tomando como buenas prácticas la

gestión de los activos, seguridad de las operaciones, gestión de incidentes, recuperación ante desastres y el control de accesos (20).

Tomando en cuenta que en esta fase es donde el cliente se involucra, es necesario tener el control del servicio, garantizando la satisfacción del cliente y que este cuente con lo requerido, mejorando la experiencia de usuario y garantizando paralelamente el cumplimiento de los objetivos del negocio.

La fase de operación se integra de los siguientes procesos:

- Gestión de eventos
- Gestión de incidencias
- Petición de servicios de TI
- Gestión de problemas
- Gestión de acceso a los servicios de TI

2.3.7. Mejora continua del servicio

Mejorar, es un concepto, incluso personal en cada individuo, que determina una etapa de cambios positivos orientados a disminuir o anular cualquier acción o resultado perjudicial, o maximizar los beneficios.

La mejora continua, es una actividad de revisión continua de la información generada por parte de la fase de operación, aquí pueden surgir nuevos servicios o cambios al servicio en operaciones. Esto implica una continua monitorización y evaluación de las actividades y procesos de los servicios (14), esto se logra estableciendo métricas y analizando los resultados de los indicadores preestablecidos.

Los elementos que componen la mejora continua de los servicios son:

- Conformidad
- Calidad
- Rendimiento
- Valor

Los resultados que se obtienen del monitoreo y evaluación sirven insumo para cotejar que estos están dentro de las especificaciones detalladas en los acuerdos de nivel de servicio (SLA's),

dando paso a mejorar la calidad, integrar nuevos servicios y aumentar la eficiencia de los procesos de negocio.

Para lograr una buena orientación de la mejora continua, se debe establecer en primera instancia que se quiere medir y como medirlo. Por ejemplo, un servicio de repartición de

Esta fase integra los procesos siguientes:

- Procesos de mejora
- Informes de servicios de TI

2.4. Seguridad de Información

2.4.1. Concepción de la seguridad de Información

En el sentido más sencillo, la Seguridad de la Información es el hecho de mantener los datos seguros y a salvo no sólo del acceso no autorizado, sino también del acceso corrupto. El principal objetivo de la seguridad de datos es garantizar que los datos estén seguros y al margen de cualquier tipo de amenaza a la seguridad. La información se almacena en las bases de datos, en las computadoras y en las redes. Si bien algunos de estos datos pueden no ser tan secretos, otros pueden tener valor e importancia lo cual requiere ser privados. Sin embargo, el acceso no autorizado a dicha información o datos privados puede causar muchos problemas, como la corrupción, la filtración de información confidencial y la violación de la privacidad.

Sabemos que hoy en día las redes de datos son importantes porque interconecta las diferentes aplicaciones para brindar un servicio por lo que es importante siempre llevar etapas para fortalecer la seguridad de esta. La primera etapa es la obtención de la mayor cantidad de información posible de la red objetivo, para ello se aplican las técnicas basadas en diferentes tipos de consultas a los servidores DNS y en el análisis de los mensajes de enrutamiento. Se destaca que en esta fase no se pretende obtener ninguna vulnerabilidad, lo que se intenta con ella es obtener una lista lo más amplia posible en los ordenadores con presencia en Internet de la red objetivo. Este listado de equipos de red se utiliza en una segunda fase denominada escaneo de puertos y enumeración de servicios, en esta fase se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos. Según el tipo de puerto y servicio que esté activo en cada equipo se puede inferir el papel que desempeña

dentro de la organización. Una vez en esta fase no se trata de encontrar ninguna vulnerabilidad, sino de determinar el equipo crítico de la red objetivo a la que se aplicará el análisis de vulnerabilidades, que es la fase final de esta metodología. Una vez obtenida la lista de equipos de red objetivo con presencia en Internet y determinada cuál de ellos desempeña un papel crítico para la red, se procede a la fase final de la metodología propuesta. Esto permitirá la evaluación de los equipos críticos en busca de vulnerabilidades. Es en esta última fase donde se realiza la evaluación de todos los servicios y los puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo. (21)

De este modo, la importancia de la seguridad de los datos entra en juego. La Seguridad de la Información se realiza en forma de medidas de privacidad digital que son aplicadas para evitar este acceso no autorizado a sitios web, redes y bases de datos. Existen muchas formas de proteger o asegurar la información que es importante y algunas de ellas incluyen el cifrado, la autenticación de usuarios, las soluciones de copia de seguridad y el borrado de datos. Hay muchas normas y estándares que rigen las medidas de seguridad de datos. Se aplican las normas de protección de datos para garantizar que los datos personales sean accesibles a las personas a las que puedan interesar.

Las estafas de phishing son normalmente mensajes de correo electrónico fraudulentos que aparentemente proceden de fuentes legítimas. Por lo general, estos mensajes lo orientan a un sitio web fraudulento para conseguir la información privada como su contraseña, tarjeta de crédito u otros detalles de la cuenta.

Es importante también educar a sus empleados sobre las tácticas de los phishers. Como parte de su formación, los empleados deben recibir formación en materia de seguridad. Informar a las personas para que tengan cuidado con los correos electrónicos con archivos adjuntos de personas que no conocen. Hacerles saber que ningún sitio web creíble les pediría su contraseña por correo electrónico, por lo que la intención de los estudios de seguridad útiles que simulen ataques a usuarios es evaluar la capacidad de los usuarios en la detección de ataques con o sin diferentes mecanismos de defensa. (22)

Si bien todo tipo de datos personales son importantes, uno de los aspectos en los que la necesidad y el requisito de seguridad de los datos son más frecuentes es en las empresas y las

industrias. La mayor parte de los negocios dependiendo de su categorización como PYMES pueden contar con una cantidad de información que pueden ser confidenciales y estar protegidos de otras personas. Con frecuencia, las empresas se esfuerzan por crear manuales de buenas prácticas de seguridad en la medida que la información sigue creciendo. Además, es difícil controlar todos los datos desde un área tecnológica ya que todas las personas deben estar involucradas. Pero se crean equipos que velan por resolver estos problemas y proporcionar una protección de datos completa.

La protección y seguridad de sus datos empresariales es fundamental tanto para su empresa como para su reputación y su equipo de empleados. ¿Conviene que un hacker desconocido arruine la empresa que ha estado formándose durante años? Por esta razón, es importante contar con el antivirus más adecuado para las empresas.

El antivirus es una opción ideal para pequeñas y medianas empresas sin departamentos de TI. Si no contrata personal para gestionar la ciberseguridad de la empresa, podrá instalar una aplicación de antivirus adecuado y disfrutar en todo momento de una protección contra programas maliciosos. De esta manera, la solución es más rentable: un programa trabaja las 24 horas del día y evita el riesgo de errores y equivocaciones, de hecho, cada uno de ellos tiene sus técnicas de detección de virus informáticos. (23)

A parte de asegurar y proteger la información, también es importante gestionarla y controlarla adecuadamente. La gestión de información es el desarrollo y la ejecución de las buenas prácticas que ayudan a todos los requisitos del ciclo de vida de los datos de una empresa. El alcance de esta concepción de la gestión de datos es muy amplio y puede aplicarse a cualquier tipo de negocio.

La gestión de la información es importante porque, sin una gestión adecuada de la información, sería difícil controlarla y protegerla. Si la información no está bien delimitada, puede ser utilizada indebidamente en diversos tipos de aplicaciones. Si la información no está bien definida, sería imposible satisfacer las necesidades de los usuarios.

La seguridad de la información es fundamental para la mayoría de las empresas. Todo tipo de información como los datos de los clientes, los datos bancarios, los datos de las cuentas, los archivos personales, etc., debe ser bien protegida, ya que, si llegan a manos equivocadas,

se pueden utilizar de forma indebida con facilidad. Esta información puede ser difícil de reemplazar y potencialmente peligrosa. Al asegurar tales datos o información, uno puede proteger los archivos y evitar enfrentar cualesquiera inconvenientes. (24)

Sabemos que hoy en día la tecnología ha ido evolucionando a nuevas formas de proporcionar facilidades de acceso a la información en la vida cotidiana y en la medida en que los dispositivos móviles son cada vez más utilizados, se han ido convirtiendo en un almacenamiento móvil que permite almacenar la información personal y empresarial de los usuarios. En la mayoría de los sistemas operativos móviles, entre ellos Android, se guardan datos personales en bases de datos y se facilitan API's para tener acceso a las aplicaciones, que se pueden utilizar para acceder a una base de datos gestionada por el sistema o para gestionar su propia base de datos. No obstante, Android, que es uno de los sistemas operativos móviles más usados, guarda los datos como texto plano en su base de datos; en consecuencia, se puede filtrar el contenido de la base de datos de forma accidental a través de varias vulnerabilidades, por lo que es importante proveer de un entorno seguro. (25)

El mejor camino para proteger los datos confidenciales es permitir que el administrador los cifre y ser el único que pueda descifrarlos correctamente. Al ofrecer a los usuarios un control total de su información, el riesgo causado por un servidor en línea en peligro puede reducirse al usar seguridad por token. (26)

Un manual de buenas prácticas apoya a cualquier empresa bajo las siguientes categorías generales:

1. **Confidencialidad:** Que la información solamente debe ser visualizada por las personas que están autorizadas a acceder a ella.
2. **Integridad:** Debe ser modificada únicamente por personas autorizadas para ello.
3. **Disponibilidad:** Se debe disponer de información cuando se necesite
4. **No Daño:** No se debe producir ningún tipo de daño en un sistema que no pueda ser rastreado hasta una persona responsable.

2.4.2. Estándares de seguridad de información

1. ISO 27001

ISO/IEC 27001, también conocida con el nombre de ISO 27001, constituye una norma de seguridad que esboza los requisitos sugeridos para construir, supervisar y mejorar un sistema de gestión de la seguridad de la información (SGSI). Es un conjunto de políticas para proteger y administrar la información confidencial de una empresa, como, por ejemplo, los datos financieros, la propiedad intelectual, los datos de los clientes y los registros de los empleados.

ISO 27001 es un estándar de cumplimiento voluntario que emplean los proveedores de servicios con el fin de proteger la información de los clientes. Implica que un ente acreditado e independiente debe auditar formalmente a una organización para asegurar su cumplimiento.

Este estándar fue creado para ofrecer a las empresas un cierto grado de protección de la seguridad de la información. La norma ISO 27001 estipula los diferentes mecanismos de control que es necesario establecer para estar al nivel de los requisitos de certificación, tales como:

1. Detectar los posibles riesgos para la seguridad de la información.
2. Brindar un entorno seguro para la implementación y gestión ideal de los controles.
3. Administrar adecuadamente el cumplimiento de las normas y reglamentos.
4. Delineando los objetivos de la gestión de la seguridad de la información.
5. Destacar las políticas, estándares y procesos de seguridad de la información que deben seguir las empresas.

2. ISO 27002

La ISO 27002 es un listado de directrices de seguridad de la información que pretenden contribuir a la implementación, mantenimiento y mejora de la gestión de la seguridad de la información de una organización.

En las recomendaciones se hace hincapié en la importancia de gestionar los derechos de acceso privilegiado para proteger la información. Como lo demuestra nuestro reciente informe sobre amenazas, esto es fundamental para frustrar los ataques avanzados. En caso de despido o renuncia, por ejemplo, los empleados o contratistas descontentos pueden utilizar sus derechos de acceso privilegiado para sabotear o corromper deliberadamente la información, y/o verse tentados a recopilar información para su uso en el futuro.

Hay controles relacionados con la seguridad de las cuentas privilegiadas en toda la norma ISO/IEC 27002, incluidos los requisitos para:

1. Elaborar y aplicar una política de acceso privilegiado
2. Identificar los derechos de acceso privilegiado asociados a cada uno de los sistemas o procesos
3. La restricción del uso del acceso privilegiado a los usuarios autorizados en función de las tareas operativas.
4. Autenticación de usuarios privilegiados, asegurando la responsabilidad individual por acciones privilegiadas.
5. Cambiar las contraseñas predeterminadas de los proveedores
6. Restringiendo el acceso a programas de utilidades privilegiadas
7. El control del acceso privilegiado de los proveedores
8. Registro y monitoreo de acceso privilegiado

3. ISO 27033

ISO/IEC 27033-1 proporciona un panorama en general de la seguridad de la red y otras definiciones relacionadas. En el mismo se definen y describen los términos relacionados con la seguridad de las redes y se proporcionan directrices de gestión al respecto entre otros. Lo dicho con anterioridad a la seguridad de la red se aplica a la seguridad de los dispositivos, la seguridad de las actividades de gestión relacionadas con los dispositivos, las aplicaciones/servicios y los usuarios finales, además de la seguridad de la información que se transfiere a través de los enlaces de comunicación.

Es importante para todos los que participan en la gestión de la red. Entre ellos se incluyen los administradores y otros cargos como gerentes o usuarios que se encarga en la gestión de la configuración o también para realizar la comunicación con los diferentes clientes, todo esto en conjunto con los gerentes y administradores que tienen responsabilidades específicas en materia de seguridad de la información y de seguridad de la red, funcionamiento de la red, o que son responsables del desarrollo de los programas de seguridad y de las políticas de seguridad de una organización en general. Además, es de interés para cualquier persona que participe en la planificación, diseño e implementación de los aspectos arquitectónicos de la seguridad de las redes.

Brinda orientación sobre cómo identificar y analizar los riesgos de seguridad de la red y la definición de los requisitos de seguridad de la red sobre la base de ese análisis.

Contiene una visión de conjunto de los controles que soportan las arquitecturas de seguridad técnica de redes e información técnica relacionada, además de los controles no técnicos y los controles técnicos que son aplicables no sólo a las redes.

Presenta cómo lograr arquitecturas de seguridad técnica de redes de buena calidad, y los aspectos de riesgo, diseño y control asociados con escenarios típicos de red y áreas de tecnología de red.

Examina brevemente las cuestiones relacionadas con la aplicación y el control de la seguridad de las redes, así como el seguimiento y la revisión en curso de su aplicación.

3. Capítulo III. Metodología de la investigación

3.1. Tipo de investigación

Basado en el enfoque del tema, se realizará un tipo de investigación mixta; el cual “implica un proceso de recolección, análisis y vinculación de datos cuantitativos y cualitativos en una misma investigación” según Sampieri (27).

Para la investigación cuantitativa, en relación con el alcance se realizará una investigación descriptiva según Sampieri (27), ya que se utilizará para describir las buenas prácticas de las metodologías TIC con mayor reconocimiento en el mercado. Además, que no se harán predicciones de aplicabilidad ni comprobaciones de hipótesis o supuestos, partiendo del hecho que una buena práctica total o parcial siempre trae resultados favorables.

Para la investigación cualitativa, la estrategia a utilizar es la teoría fundamentada en base al contexto de estudio según Creswell (28).

En cuanto a la metodología se establece que las unidades de análisis corresponden a la investigación cuantitativa y el sujeto de estudio a la investigación cualitativa.

Las unidades de análisis tienen una relación con las variables cuantitativas, y el sujeto de estudio es quién permite determinar los puntos de investigación que conlleva un resultado cualitativo.

3.2. Unidades de análisis

En base al objetivo específico “analizar cada una de las partes integradas por las metodologías TIC más reconocidas”, se cuentan con las unidades de análisis:

- Infraestructura de TI
- Servicios TI
- Sistemas informáticos
- Seguridad.

Para el objetivo específico “evaluar cada metodología basada en la dimensión del sector micro y pequeña empresa en El Salvador”, se tienen las unidades de análisis:

- Requisitos indispensables de cada metodología y criterios de clasificación de micro y pequeña empresa.

Finalmente, con el objetivo específico “consolidar las buenas prácticas TIC aplicables a la micro y pequeña empresa en El Salvador”, se cuenta con las unidades de análisis:

- Buenas prácticas
- Modelo de aplicación de buenas prácticas.

3.3. Sujeto de estudio

En base al objetivo específico “evaluar cada metodología basada en la dimensión del sector micro y pequeña empresa en El Salvador”, se cuenta con el sujeto de estudio:

- Experto implementador de metodologías TIC que cumpla con el siguiente perfil:
 - Formación académica referente a la rama de la informática.
 - Conocimiento de los requisitos y aplicación de la norma ISO 27001 y las metodologías COBIT e ITIL.
 - Al menos 3 años de experiencia en el ámbito de las TIC.

Para el objetivo dos y tres no se consideraron sujetos de estudio, ya que metodológicamente el alcance de los mismos es cuantitativo.

3.4. Variables y su medición

Para las variables se ha definido usar la técnica de análisis de contenido y son las siguientes:

- Hardware
- Comunicación de datos
- Administración
- Software
- Riesgo
- Estructura Organizativa
- Financiero
- Guía de criterios aplicables
- Aplicabilidad
- Presupuesto

Para dichas variables se utilizó dicha técnica por que el análisis de contenido es un método de investigación que permite estudiar documentos y artefactos de comunicación, los cuales pueden ser textos de varios formatos, pero en nuestro estudio siempre nos apoyamos en fuente fidedignas. Uno de los principales puntos fuertes del análisis de contenidos es su carácter no invasivo, en contraposición a la simulación de experiencias sociales o la recopilación de respuestas a encuestas.

También se ha considerado usar para la siguiente variable:

- Resultados de implementación de la metodología TIC la técnica de la entrevista.

La variable mencionada anteriormente se ha usado la técnica de entrevista porque se desarrolla la relación entre el entrevistador y el entrevistado por medio de una entrevista. Mejora la comprensión mutua y la cooperación entre las partes, por lo que todo malentendido y error puede rectificarse con facilidad en una entrevista porque el entrevistador y el entrevistado se encuentran físicamente presentes ante el comité de entrevistas.

3.5. Procedimiento y análisis

La investigación cuenta con las siguientes unidades de análisis:

- Infraestructura de TI, utilizarán las variables Hardware y comunicación de datos a través de la técnica análisis de contenido utilizando un cuadro resumen (ver instrumento 1 en los anexos A.1.1 y A.1.2.)
- Servicios de TI, utilizará la variable de Administración a través de la técnica análisis de contenido utilizando un cuadro resumen (ver instrumento 3 en los anexos A.1.3).
- Sistemas informáticos, utilizará la variable Software a través de la técnica análisis de contenido utilizando un cuadro resumen (ver instrumento 4 en los anexos A.1.4).
- Seguridad, utilizará la variable de Riesgo a través de la técnica análisis de contenido utilizando un cuadro resumen (ver instrumento 5 en los anexos A.1.5).
- Requisitos indispensables de cada metodología, utilizará la variable de los Requisitos a través de la técnica análisis de contenido utilizando la documentación de la metodología como instrumento (ver instrumento 6 en los anexos A.1.6).
- Criterios de clasificación de micro y pequeña empresa, utilizarán las variables, utilizará la variable de la estructura organizativa y financiero a través de la técnica análisis de contenido utilizando un cuadro resumen (ver instrumento 7 en los anexos A.1.7 y A.1.8).
- Experto implementador de metodología TIC, utilizará la variable de la variable resultados de implementación de metodologías TIC a través de la técnica entrevista utilizando un guion de entrevista (ver instrumento 9 en los anexos A.1.9).
- Estado del arte, utilizará la variable guía de criterios aplicables a través de la técnica análisis de contenido utilizando un cuadro de clasificación (ver instrumento 10 en los anexos A.1.10).
- Buenas prácticas, utilizará la variable aplicabilidad a través de la técnica análisis de contenido utilizando una lista de chequeo de buenas prácticas (ver instrumento 11 en los anexos A.1.11).

- Modelo de aplicación, utilizará la variable presupuesto a través de la técnica análisis de contenido utilizando un matriz de costos (ver instrumento 12 en los anexos A.1.12).

4. Capítulo IV. Resultados

La investigación cuenta con los siguientes resultados en las unidades de análisis:

Objetivo	Variable	Resultados
Analizar cada una de las partes integradas por las metodologías de TIC más reconocidas	Hardware	Los resultados de la unidad de análisis de la Infraestructura de TI, utilizando las variables Hardware y comunicación de datos a través de la técnica análisis de contenido usando un cuadro resumen (ver resultados del instrumento 1 y 2 en los anexos A.2.1 y A.2.2.)
	Servicios TI	Los resultados de la unidad de análisis de los Servicios de TI, empleando la variable de Administración a través de la técnica análisis de contenido usando un cuadro resumen (ver resultados del instrumento 3 en los anexos A.2.3).
	Sistemas informáticos	Los resultados de la unidad de análisis de los Sistemas informáticos, utilizando la variable Software a través de la técnica análisis de contenido usando un cuadro resumen (ver resultados del instrumento 4 en los anexos A.2.4).

	Seguridad	Los resultados de la unidad de análisis de la Seguridad, usando la variable de Riesgo a través de la técnica análisis de contenido utilizando un cuadro resumen (ver resultado del instrumento 5 en los anexos A.2.5).
Evaluar cada metodología basada en la dimensión del sector micro y pequeña empresa en El Salvador.	Requisitos	Los resultados de la unidad de análisis de Requisitos indispensables de cada metodología, usando la variable de los Requisitos a través de la técnica análisis de contenido utilizando la documentación de la metodología como instrumento (ver resultado del instrumento 6 en los anexos A.2.6).
	Estructura organizativa	Los resultados de la unidad de Criterios de clasificación de micro y pequeña empresa, utilizando las variables de la estructura organizativa a través de la técnica análisis de contenido usando un cuadro resumen (ver resultado del instrumento 7 en los anexos A.2.7 y A.2.8).
	Financiero	Los resultados de la unidad de Criterios de clasificación de micro y pequeña empresa, utilizando la variable financiero a través de la técnica análisis de contenido usando un cuadro resumen (ver resultado del instrumento 7 en los anexos A.2.7 y A.2.8).

Enumerar las buenas prácticas de TIC aplicables a la micro y pequeña empresa en El Salvador.	Resultados de implementación de metodologías TIC	Los resultados de la unidad de análisis de Experto implementador de metodología TIC, utilizando la variable de resultados acerca de la implementación de metodologías TIC a través de la técnica entrevista usando un guion de entrevista (ver resultado del instrumento 9 en los anexos A.2.9).
	Guía de criterios aplicables	Los resultados de la unidad del Estado del arte, utilizando la variable guía de criterios aplicables a través de la técnica análisis de contenido usando un cuadro de clasificación (ver resultado del instrumento 10 en los anexos A.2.10).
	Aplicabilidad	Los resultados de la unidad de análisis de las Buenas prácticas, utilizando la variable aplicabilidad a través de la técnica análisis de contenido usando una lista de chequeo de buenas prácticas (ver resultado del instrumento 11 en los anexos A.2.11).
	Presupuesto	Los resultados de la unidad de análisis del Modelo de aplicación, utilizando la variable presupuesto a través de la técnica análisis de contenido usando un matriz de costos (ver resultado del instrumento 12 en los anexos A.2.12).

5. Capítulo V. Modelo de buenas prácticas

Basados en los resultados obtenidos a través de las diferentes herramientas de evaluación aplicadas las metodologías seleccionadas, se ha elaborado el modelo de buenas prácticas aplicables a la micro y pequeña empresa.

Para iniciar con el desarrollo del modelo se realizó un análisis de contenido de todas las partes integradas en cada metodología, cuyo objetivo fue listar todos aquellos requisitos, sugerencias o recomendaciones de cada una, categorizándolas por las siguientes áreas de interés:

- Infraestructura de TI
- Servicios de TI
- Sistemas informáticos
- Seguridad

Luego de categorizadas, se procede a tomar únicamente aquellas sugerencias, recomendaciones o requisitos de carácter obligatorio de cada metodología, los cuales se consideran los mínimos que se deben cumplir para implementarlas, teniendo como resultado un listado filtrado con lo esencial de cada.

Con el listado de buenas prácticas se procede a realizar un cuadro de verificación donde se establecen que requisitos aplican o no aplican a la micro y pequeña empresa, esto basado en los datos de clasificación financiera y organizativa de ellas, esto reduce el listado de requisitos y deja un conglomerado de buenas prácticas aplicables a ambas, cuyo objetivo principal es que sean aplicables en la administración de los servicios de tecnología, y que se pueda llevar a cabo por partes o de manera completa.

Para revisión del modelo final, dirigirse al anexo A.3.

6. Capítulo VI. Conclusiones y recomendaciones

- Con base en el objetivo 1, el cual procuraba el análisis de cada una de las partes integradas por las metodologías de TIC mas reconocidas, se concluye que:

- Las normas y estándares de calidad mencionadas en el presente trabajo no sólo se limitan a establecer las reglas del juego, sino que además cumplen con la función de asegurar una concordancia económica que evite el incremento de los costos y de los gastos de operación de las empresas. Por lo tanto, las normas y estándares internacionales persiguen el doble objetivo de definir la ruta hacia el progreso, protegiendo al mismo tiempo los intereses de su actividad empresarial. Aunque hay otras, las normas y estándares internacionales ISO; COBIT e ITIL han sido las más reconocidas y aceptadas por las empresas porque han comprobado su utilidad real en todos los ámbitos de la actividad.
- El factor clave de diferencia entre ISO 27000 y COBIT es que el primero es exclusivamente para el propósito de la seguridad de la información, y en el segundo es para la gestión y gobierno de los procesos de negocio de la tecnología de la información. Se puede considerar COBIT como un conjunto que se centra en la gestión de la tecnología de la información (TI) y la gobernanza. COBIT no solamente habla de la seguridad en una empresa, pero también incluye la manera en que una empresa organiza, ordena y supervisa la organización de las operaciones de TI. Las normas ISO 27000, por el contrario, es una norma internacional para los sistemas de gestión de la seguridad de la información. Se enfoca en la realización de una evaluación de riesgos y luego en la aplicación de controles de seguridad específicos para la protección de los activos de información crítica de la organización. ITIL tiene como objetivo lograr la excelencia en la gestión de servicios de TI.
- En atención al objetivo 2, el cual evalúa cada metodología basada en la dimensión del sector micro y pequeña empresa en El Salvador, se concluye que:
 - La adopción de las normas ISO, ITIL Y COBIT tiene numerosos beneficios para las medianas y pequeñas empresas, son un instrumento de análisis, definición y mejora de los procesos básicos de negocio, es decir, aquellos que afectan directamente a la calidad que los clientes perciben y, por lo tanto, a la rentabilidad presente y futura de la empresa.

- Sin un grupo de personas que trabajen con un objetivo común no existe un sistema de gestión eficaz, y para que esto sea posible es necesario el liderazgo de los dueños o socios involucrados. El Sistema de Gestión de Calidad debe estar integrado por los requisitos de los procesos esenciales de la organización y sus objetivos deben formar parte de la planificación estratégica. Para conseguir este alineamiento, es fundamental la implicación de la alta dirección y su capacidad para implicar a otras personas en la eficacia de su trabajo.
- En referencia al objetivo 3, que consolida las buenas prácticas de TIC aplicables a la micro y pequeña empresa en El Salvador, se concluye que:
 - En función de la magnitud de las tareas a realizar, se recomienda nombrar a una sola persona o a un equipo especializado para que trabaje en ellas. No obstante, hay una serie de funciones mínimas que el administrador debe realizar entre ellas están realizar un diagnóstico de la situación actual de la empresa con la finalidad de evaluar y hacer un análisis de todas las necesidades de capacidad necesarias para la implementación y el manejo posterior del proyecto, es importante reconocer que es importante lograr todos los recursos económicos, humanos y tecnológicos necesarios para la certificación ISO, y luego llevar a cabo un control, seguimiento y verificación de todas las sugerencias implementadas por las normas en marcha.
 - Para un correcto control y supervisión del funcionamiento de las buenas prácticas TIC será indispensable planificar revisiones periódicas (trimestral o semestral); la priorización de las áreas a revisar debe estar debidamente acordada o basada en los procesos estratégicos del negocio.
 - Las buenas prácticas son el resultado de un grupo de procedimientos en un entorno profesional, probados y aceptados generalmente en la mayoría de las empresas del sector, que sirven para añadir valor al negocio y La gestión de los riesgos derivados del uso de los servicios de TI se realiza de forma eficiente.

Las recomendaciones en base a la investigación realizada son las siguientes:

- Es necesario contar con al menos una persona que esté relacionada con los conceptos de TIC, de ser posible un especialista que cuente con estudios orientados a la administración de TI, ya que se podrá obtener una mayor claridad, continuidad, verificación y aplicabilidad de las buenas prácticas contenidas en el manual. De no poder contar con un elemento de forma directa, se puede optar por la contratación de un servicio externo que lleve a cabo estas actividades estableciendo planes de implementación y revisión periódicas que no impliquen un costo alto para la empresa.
- La implementación de las buenas prácticas integradas en el manual puede llevarse a cabo por secciones, permitiendo un ciclo de mejora continua que permita planificar su ejecución, llevar a cabo su implementación en los procesos de negocio, revisar los resultados que se obtienen una vez implementado y tomar acciones correctivas ante situaciones que contravienen a los esperado.
- Tomar conciencia sobre la importancia de la administración de los servicios TIC con los que la empresa cuenta y el valor que estos aportan a sus procesos de negocio, los cuales se verán maximizados con la aplicación de cada una de las buenas prácticas contenidas en el manual.
- Llevar a cabo un análisis de situación actual que ponga en perspectiva con lo que se cuenta, su valor al negocio y los procesos en los que se ven involucrados. Una vez obtenido, se pueden aplicar las buenas prácticas para determinar si los recursos actuales están debidamente alineados al negocio y que sean los necesarios para llevar a cabo las operaciones del negocio, permitiendo disponibilidad, continuidad y escalabilidad ante el crecimiento del negocio.
- La implicación de la Administración de la empresa es necesaria no sólo porque la normas TIC lo requiere como requisito, sino porque de ella dependen los recursos humanos, técnicos y financieros que se necesitan para llevar a cabo el trabajo a realizar. De esta manera, el compromiso de la Administración se refleja en la agilización de la política de calidad, en la comunicación de la misma a los empleados y fomenta la sensibilización sobre los objetivos y las metas que la organización quiere alcanzar.

- En una primera etapa, la ejecución sólo necesita el compromiso del personal de alta dirección y del personal clave que actúa como gestores. Pero una vez que el proyecto avanza, es necesario nombrar un equipo completo de implementación: Delegado de Administración, Coordinadores, Supervisores, Representantes de todas las áreas de la organización que para empresas PYMES se requiere de un analista que tenga el conocimiento sufriendo lo mencionado anteriormente, y dedicado a registrar todos los eventos durante la implementación del Sistema de Gestión de Calidad.
- Hay que diseñar e implementar programas de sensibilización en el documento de las buenas prácticas, ya que es un mecanismo efectivo para transmitir a los empleados el objetivo y los beneficios de un Sistema de Gestión de la Calidad basado en las normas TIC más utilizadas a nivel empresarial. De esta forma, cada una de las partes interesadas que constituyen la empresa entenderán los beneficios de llevar a cabo cada uno de esos puntos reduciendo riesgos y ser más eficientes para la organización, entendiendo los distintos niveles de participación en la ejecución y las ventajas que el aseguramiento de la calidad se ofrece a sí misma.
- Cuando se comprenden que la implementación de las sugerencias de las normas TIC afecta a todas las áreas. Los profesionales de las diferentes áreas de la empresa no necesariamente tienen que conocer la esencia que comprenden las normas. Pero es evidente que la formación y el entrenamiento son parte esencial de la implantación y los buenos resultados.
- Lo cierto es que, en el momento de entrar en vigor con las buenas prácticas, resulta imprescindible saber la efectividad de los mismos y conocer los posibles fallos que pueda presentar. La mejor manera de hacerlo es a través de una Auditoría Interna con la finalidad de validar el cumplimiento

Bibliografía

1. *Buenas practicas en el uso de las TIC en universidades ecuatorianas*. Wladimir, Paredes-Parada. 2018.
2. *Adoption problems of information technology service management models*. Meléndez-Llave, Karin Ana y Dávila-Ramón, Abraham Eliseo. 2018.
3. **CONAMYPE**. *Encuesta Nacional de la Micro y Pequeña Empresa 2017 Con el apoyo financiero de: Fondo Especial de los Recursos Provenientes de la Privatización de la Administración Nacional de Telecomunicaciones (FANTEL)*. Julio : 2019, 2017. 20.
4. —. Política Nacional para el Desarrollo de la Micro y Pequeña Empresa. [En línea] 28 de Noviembre de 2017. [Citado el: 2 de Agosto de 2019.] <https://www.conamype.gob.sv/download/politica-nacional-para-el-desarrollo-de-la-micro-y-pequena-empresa/>.
5. —. Ley MYPE. [En línea] [Citado el: 2 de Agosto de 2019.] <https://www.conamype.gob.sv/temas-2/ley-mype/>.
6. Orellana, Javier. La prensa grafica. [En línea] 20 de Julio de 2018. [Citado el: 2 de Agosto de 2019.] <https://www.laprensagrafica.com/economia/Cuantas-microempresas-hay-en-El-Salvador-20180720-0042.html>.
7. **CONAMYPE**. Estrategia para la inclusión digital de la MYPE. **CONAMYPE**. [En línea] Noviembre de 2016. [Citado el: 20 de Julio de 2019.] <https://www.conamype.gob.sv/wp-content/uploads/2016/11/Estrategia-Digital.pdf>.
8. Saavedra, John y Torres Olaya, Alfonso. Universidad ICESI. [En línea] 2012. [Citado el: 14 de Marzo de 2019.] https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/70808/1/modelo_gobierno_procesos.pdf.
9. Quintanilla, Gloria. Software Guru. *Introducción a COBIT 5*. [En línea] [Citado el: 10 de Julio de 2019.] <https://sg.com.mx/sgce/2013/sessions/introducci%C3%B3n-cobit-5>.
10. Gutiérrez Amaya, Camilo. COBIT como guía para integrar la operación de TI. *welivesecurity*. [En línea] 2013. [Citado el: 17 de Abril de 2019.] <https://www.welivesecurity.com/la-es/2013/06/18/cobit-como-guia-para-integrar-operacion-ti/>.
11. Macgregor, Stuart. Mapping TOGAF and COBIT. [En línea] [Citado el: 29 de Mayo de 2012.] <http://www.google.com.co/url?sa=t&rct=j&q=macgregor%20%20stuart%20%22ma>.
12. COBIT "Objetivos de Control para la Información y la Tecnología relacionada". [En línea] 19 de Marzo de 2017. [Citado el: 10 de Febrero de 2019.] <http://cobitzd.blogspot.com/2017/03/dominios.html>.
13. COBIT. [En línea] 26 de Marzo de 2017. [Citado el: 10 de Febrero de 2019.] <http://cobitmmatiasc.blogspot.com/2017/03/dominios-y-procesos-de-cobit.html>.

14. Bailey, Cristian. *ITIL Version 3, manual técnico de fundamentos*. 2010.
15. Cruz Hinojosa, Nancy Judith. ITIL: Cómo aplicar las buenas prácticas en las PYMEs. *tic.portal*. [En línea] 2017. [Citado el: 12 de Abril de 2019.] <https://www.ticportal.es/expert/itil-buenas-practicas-pymes>.
16. *How small and medium enterprises can begin their implementation of ITIL*. Calvo-Manzano, Jose Antonio, y otros. 2015.
17. *The Relationship between KM strategies and IT applications in SMEs*. Azyabi, Naie, y otros. 2014.
18. *La influencia de la implementación de las TIC en la productividad de empresas de servicios*. Arévalo-Avecillas, Danny, Nájera-Acuña, Santiago y Piñero, Edgar. 2018.
19. *Review of Proposals for the construction and management of the catalog of IT Services*. MERA MACIAS, CRISTIAN y AGUILAR ALONSO, IGOR. 2018.
20. INCIBE. Buenas prácticas en el área informática. Colección: Protege tu empresa. [En línea] 15 de Febrero de 2019. [Citado el: 28 de Abril de 2019.]
21. *Metodología para la Detección de Vulnerabilidades en Redes de Datos*. A, Franco David, L., Perea Jorge y Plinio, Puello. 2012.
22. *Conducting ethical yet realistic usable security studies*. Amir, Herzberg y Ronen, Margulies. 2013.
23. *Análisis comparativo de los principales sistemas antivirus*. Armas Montesinos, Luis. 2003.
24. *A Data-Driven Security Risk Assessment Scheme for Personal Data Protection*. Cha, Shi-Cho y Yeh, Kuo-Hui. 2018.
25. *Security Architecture for a Secure Database on Android*. Hyung, Park Jin, y otros. 2017.
26. *Secureweb: Protecting sensitive information through the web browser extension with a security token*. Shuang, Liang, y otros. 2018.
27. Hernandez Sampieri, Roberto. *Metodología de la investigación*. Cuarta edición. s.l. : McGraw-Hill Interamericana.
28. Creswell, John W. *Research design*. Tercera edición.
29. Banerjee, R. Tips for Making COBIT 5 Implementation Fit the Enterprise. [En línea] 2018. [Citado el: 20 de Marzo de 2019.] <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=130404891&lang=es&site=ehost-live>.
30. Ferrer Olivares, Fernando. Consideraciones prácticas para una implementación exitosa. [En línea] 2011. [Citado el: 12 de Abril de 2019.] <https://www.proactivanet.com/UserFiles/File/FERROLIG-TCM-COBIT.pdf>.

31. Ibana, Yuichi (Rich). *Creating Value with an Enterprise IT Governance Implementation Model Using COBIT 5*. [En línea] 2016. [Citado el: 21 de Abril de 2019.] <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=115719348&lang=es&site=ehost-live>.
32. ISACA. http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf. ISACA. [En línea] [Citado el: 4 de Mayo de 2019.] http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf.
33. Jayaraman, Sudarsan. *Why, When and How to Migrate to COBIT 5*. [En línea] 2013. [Citado el: 4 de Mayo de 2019.] <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=89579594&lang=es&site=ehost-live>.
34. L., Roberto. *EL CONTROL INTERNO EN LAS PYMES: UN ENFOQUE SIMPLIFICADO DEL COSO I Y COSO II. PÍLDORAS EMPRESARIALES*. [En línea] 29 de Febrero de 2016. [Citado el: 6 de Mayo de 2019.] <https://pildorasempresariales.wordpress.com/2016/02/29/el-control-interno-en-las-pymes-un-enfoque-simplificado-del-coso-i-y-coso-ii/>.
35. *IT Governance Effectiveness and its antecedents - an Empirical Examination in Brazilian Firms*. Lerch Lunardi, Guilherme, G. Maçada, Antonio Carlos y Luiz Becker, João. 2014.
36. *¿Qué puede aprender Latinoamérica del auge de Las tic en el Asia pacífico?* López, Pablo y Rosado, Luis. 2013.
37. Maigua, Gustavo y López, Enmanuel. *Buenas practicas en la dirección y gestión de proyectos informáticos*. Argentina : Universidad Tecnológica Nacional, 2012.
38. *Aprendizaje, innovación y gestión tecnológica en la pequeña empresa. Un estudio de las industrias metalmecánica y de tecnologías de información en Sonora*. Mendoza León, Jorge y Valenzuela Valenzuela, Alejandro. 2014.
39. *Estrategias para fortalecer capacidades de innovación: una visión desde micro y pequeñas empresas*. Morales Rubiano, María Eugenia, y otros. 2016.
40. Núñez, Gustavo . *Gobierno de tecnologías de información, un enfoque para las PYMES*. 2015.
41. Ojeda, Marcia. *ITIL y COBIT para el Cumplimiento de TI en PYMES: Ciclo de Vida de Servicio*. *gbadvisors*. [En línea] [Citado el: 5 de Julio de 2019.] <https://www.gb-advisors.com/es/itil-cobit-cumplimiento-de-ti/>.
42. Oparaugo, C. *COBIT 5 Mapping Exercise for Establishing Enterprise IT Strategy*. [En línea] 2016. [Citado el: 5 de Julio de 2019.] <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=120048625&lang=es&site=ehost-live>.

43. Radhakrishnan, Sreechith. 5 Common Mistakes in Adopting COBIT 5. *ISACA*. [En línea] [Citado el: 21 de Julio de 2019.] <http://www.isaca.org/COBIT/focus/Pages/5-common-mistakes-in-adopting-cobit-5.aspx>.
44. Rubio Sánchez, Juan Luis y Burgos García, Concepción. Metodología de selección de procesos para la gestión de servicios en las pymes. [En línea] 2017. [Citado el: 21 de Julio de 2019.] <https://dialnet.unirioja.es/descarga/articulo/6159618.pdf>.

Anexos

A.1 Instrumentos de medición

A.1.1 Instrumento 1

Unidad de análisis:	Infraestructura de TI.				
Variable:	Hardware.				
Técnica:	Análisis de contenido.				
Instrumento:	Cuadro resumen.				
Objetivo:	El instrumento pretende consolidar las políticas de hardware establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.				
Cuadro resumen					
Metodología / Hardware	Adquisición de equipos	Renovación de equipos	Uso de los equipos	Inventario de equipos	Reparación de equipos
ITIL					
COBIT					
ISO 27000					

A.1.2 Instrumento 2

Unidad de análisis:	Infraestructura de TI.			
Variable:	Comunicación de datos.			
Técnica:	Análisis de contenido.			
Instrumento:	Cuadro resumen.			
Objetivo:	El instrumento pretende consolidar las políticas de comunicación de datos establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.			
Cuadro resumen				
Metodología / Comunicación de datos	Adquisición de servicios de comunicación	Estándar de comunicación	Políticas de acceso a información	Redes informáticas
ITIL				
COBIT				
ISO 27000				

A.1.3 Instrumento 3

Unidad de análisis:	Servicios TI.			
Variable:	Administración.			
Técnica:	Análisis de contenido.			
Instrumento:	Cuadro resumen.			
Objetivo:	El instrumento pretende consolidar las políticas de administración de TI establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.			
Cuadro resumen				
Metodología / administración	Cuentas de correo electrónico	Asignación de equipo informático	Priorización de recursos	Administración de equipos
ITIL				
COBIT				
ISO 27000				

A.1.4 Instrumento 4

Unidad de análisis:	Sistemas informáticos.						
Variable:	Software.						
Técnica:	Análisis de contenido.						
Instrumento:	Cuadro resumen.						
Objetivo:	El instrumento pretende consolidar las políticas de software establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.						
Cuadro resumen							
Metodología / software	Licenciamiento	Inventario	Respaldos de la información	Usuarios	Desarrollo de software	Adquisición de software	Renovación de software
ITIL							
COBIT							
ISO 27000							

A.1.5 Instrumento 5

Unidad De Análisis:	Seguridad			
Variable:	Riesgo			
Técnica:	Análisis de contenido			
Instrumento:	Cuadro resumen			
Objetivo:	El instrumento nos permite medir los controles que están tomando para la seguridad de las empresas			
	Cuadro resumen			
Metodología	Actualización Aplicaciones	Protección antivirus y análisis periódico.	Realizar Copias de seguridad	Controles de acceso
ITIL				
COBIT				
ISO27000				

A.1.6 Instrumento 6

Unidad De Análisis:	Requisitos indispensables de cada metodología
Variable:	Requisitos
Técnica:	Análisis de contenido
Instrumento:	Cuadro resumen
Objetivo:	

El instrumento nos permite tomar en consideración los requisitos para cada normativa

	Cuadro resumen		
	ITIL	COBIT	ISO27000
Requisitos			

A.1.7 Instrumento 7

Unidad de análisis:	Criterios de clasificación de micro y pequeña empresa		
Variable:	Estructura organizativa		
Técnica:	Análisis de contenido		
Instrumento:	Cuadro resumen		
Objetivo:	El instrumento utilizado como cuadro resumen es para conocer parte del carácter de cualquier tipo de empresa. Por lo tanto, la importancia de la estructura organizativa nos ayuda a conocer como base de la propia cultura organizativa.		
	Cuadro resumen		
	Número de empleados	Ubicación geográfica	Rubro de la empresa
			Autoridad central o descentralizada
Microempresa			
Pequeña Empresa			

A.1.8 Instrumento 8

Unidad De Análisis:	Criterios de clasificación de micro y pequeña empresa		
VARIABLE:	Financiero		
Técnica:	Análisis de contenido		
Instrumento:	Cuadro resumen		
Objetivo:	Determinar la inversión destinada al área de tecnología		
	Cuadro resumen		
		Capital de la Empresa	Presupuesto TI
	Microempresa		
	Pequeña Empresa		

A.1.9 Instrumento 9

Unidad de análisis:	Experto implementador de metodologías TIC
Variable:	Resultados de implementación de metodologías
Técnica:	Entrevista
Instrumento:	Guion de entrevista
Objetivo:	Conocer los resultados que se pueden obtener a través de la implementación de buenas prácticas tomadas de las metodologías ITIL, COBIT e ISO 27001.
Guion de entrevista	
Buen día, se agradece la oportunidad de poder realizar la siguiente entrevista. Mi nombre es _____, el motivo de esta reunión es para realizarle algunas preguntas con respecto a las metodologías de tecnologías de información y comunicación (TIC) que ha llevado a cabo y a su vez conocer los beneficios de su implementación. 1. ¿Cuántos años de experiencia tiene en el ámbito informático? 2. ¿Ha implementado en su trabajo u otros lugares alguna metodología de TIC, tales como COBIT, ITIL o ISO 27001? Si su respuesta es no, pasar a la pregunta 9: 3. ¿Qué metodologías ha implementado? 4. ¿Cuáles han sido los motivos por los que ha optado por implementarlas? 5. ¿La implementación ha sido apoyada por la alta gerencia, o se ha llevado a cabo por iniciativa propia? 6. ¿Ha tomado como referencia algunas partes de las metodologías considerándolas buenas prácticas, o todas se han llevado a cabo con la finalidad de una implementación completa?	

7. En base a su experiencia ¿Cuál o cuáles considera que son las áreas principales a las que se deben aplicar metodologías TIC?
8. Considerando la situación antes de aplicar una metodología ¿Cuáles han sido los resultados obtenidos a la fecha?
9. ¿Qué otras metodologías conocen?
10. Para el caso de micro y pequeña empresa ¿Sería posible implementar parte de las buenas prácticas que las metodologías ofrecen?
11. ¿Considera que hay buenas prácticas de estas metodologías que no requieren un conocimiento especializado en TIC?
Si la respuesta es sí: ¿Puede mencionarnos algunos ejemplos?
Si la respuesta es no: ¿Cuánto es el costo de una persona con conocimientos mínimos de tecnologías?
12. ¿Considera usted que estas metodologías tienen prácticas que no requieren un costo a quien lo implementa, más que únicamente el esfuerzo de llevarla a cabo?
Si la respuesta es sí: ¿Podría mencionarnos algunos ejemplos?
Si la respuesta es no: ¿Podría mencionarnos algunos ejemplos de costos incurridos?

Gracias por el tiempo otorgado, la información que nos ha brindado es de total confidencialidad y será de mucha utilidad para el análisis de nuestro trabajo de graduación.

A.1.10 Instrumento 10

Unidad de análisis:	Estado del arte					
Variable:	Guía de criterios					
Técnica:	Análisis de contenido					
Instrumento:	Cuadro de clasificación					
Objetivo:	Clasificar las buenas prácticas encontradas como obligatorias en las metodologías para una mayor comprensión y segmentación de áreas de aplicación.					
Guía de criterios						
Metodología	Administración de hardware	Administración de software	Seguridad	Administración de servicios de tecnología	Recursos humanos	Gestión del conocimiento
ITIL						
COBIT						
ISO 27000						

A.1.11 Instrumento 11

Unidad de análisis:	Buenas prácticas		
Variable:	Aplicabilidad		
Técnica:	Análisis de contenido		
Instrumento:	Lista de chequeo de buenas prácticas		
Objetivo:	Identificar aquellas buenas prácticas que son aplicables a la micro y pequeña empresa, basados en su clasificación.		
Lista de chequeo de buenas prácticas			
Buena práctica	Microempresa Aplica (A) / No aplica (NA)	Pequeña empresa Aplica (A) / No aplica (NA)	Anotaciones

A.1.12 Instrumento 12

Unidad de análisis:	Modelo de aplicación
Variable:	Presupuesto
Técnica:	Análisis de contenido
Instrumento:	Matriz de costos
Objetivo:	Realizar una estimación del costo de la implementación completa de este modelo.
Matriz de costos	
Buena práctica	Costo de implementación mínimo (\$)

A.2 Instrumentos de medición completados

A.2.1 Instrumento 1

Unidad de análisis:	Infraestructura de TI.				
Variable:	Hardware.				
Técnica:	Análisis de contenido.				
Instrumento:	Cuadro resumen.				
Objetivo:	El instrumento pretende consolidar las políticas de hardware establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.				
Cuadro resumen					
Metodología / Hardware	Adquisición de equipos	Renovación de equipos	Uso de los equipos	Inventario de equipos	Reparación de equipos
ITIL	Debe evaluar costos reales asociados a la prestación de servicios Llevar la contabilidad de los gastos asociados Debe elaborarse un presupuesto Plan de inversión Ofertas de servicios de otros proveedores	Debe elaborarse un presupuesto Plan de inversión Definir si es un servicio esencial Definir si es un servicio de soporte Evaluación de externalización del servicio	Monitorear los recursos mediante los SLA Monitorear la disponibilidad evaluando el tiempo esperado versus tiempo de interrupción	Elaborar política de seguridad	Debe elaborarse un presupuesto Definir si es un servicio esencial Definir si es un servicio de soporte Evaluación de externalización del servicio Revisión del SLA

	Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio Definir si es un servicio esencial Definir si es un servicio de soporte Evaluación de externalización del servicio Elaboración de un SLA Elaboración de contratos de soporte Elaboración del plan de capacidad Elaborar manual de requisitos de disponibilidad del negocio	Revisión del SLA Revisión de contratos de soporte Revisión del plan de capacidad Elaborar manual de requisitos de disponibilidad del negocio Evaluación de riesgos contra la continuidad del servicio Evaluación de riesgos contra la continuidad del servicio Plan de recuperación Elaborar política de seguridad	Elaborar política de seguridad	Revisión de contratos de soporte Evaluación de riesgos contra la continuidad del servicio Plan de recuperación Elaborar política de seguridad
--	--	--	---------------------------------------	---

	Evaluación de riesgos contra la continuidad del servicio Plan de recuperación Elaborar política de seguridad				
COBIT	Las organizaciones deben contar con procesos para adquirir e implementar infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un	Las organizaciones deben contar con procesos para actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de	Las organizaciones deben contar con un manual el cual establezca el uso del hardware por los usuarios. En dicho manual se deben establecer lo que cada usuario puede o no realizar con el equipo, así como de penalizaciones en caso de incumplir las	Las organizaciones deben determinar la dirección tecnológica, mediante la creación de un plan de infraestructura tecnológica el cual considere el número de equipos de TI con los que cuente la empresa.	Las organizaciones deben evaluar el desempeño del hardware actual, a fin de establecer un plan de renovación de equipos.

	soporte tecnológico continuo para las aplicaciones del negocio. Se deben suministrar recursos de hardware de TI. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.	desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.	normas establecidas.		
--	--	--	-----------------------------	--	--

ISO 27000	Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización. Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica,	Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica, información de la organización.	Los requisitos de seguridad de la información deben ser definidos y consensuados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica, información de la organización.	Los activos e instalaciones asociados con la información y el procesamiento de la información han de identificarse, y se ha de diseñar y mantener un inventario de dichos activos. Los bienes inventariados deben asignarse a un propietario. Se deben aplicar, documentarse y ejecutarse normas para la utilización aceptable de la información y los bienes	Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica. El equipo de mantenimiento debe ser adecuadamente atendido para asegurar una disponibilidad e
-----------	--	--	---	--	--

	información de la organización.			relacionados con las instalaciones de tratamiento de la información. Todos los empleados y los usuarios internos y externos deberán devolver todos los activos de la organización en su poder al término de su empleo, contrato o acuerdo.	integridad continuas. Los equipos no pueden ser retirados de su lugar sin autorización previa.
--	---------------------------------	--	--	--	--

A.2.2 Instrumento 2

Unidad de análisis:	Infraestructura de TI.			
Variable:	Comunicación de datos.			
Técnica:	Análisis de contenido.			
Instrumento:	Cuadro resumen.			
Objetivo:	El instrumento pretende consolidar las políticas de comunicación de datos establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.			
Cuadro resumen				
Metodología / Comunicación de datos	Adquisición de servicios de comunicación	Estándar de comunicación	Políticas de acceso a información	Redes informáticas
ITIL	Debe evaluar costos reales asociados a la prestación de servicios Llevar la contabilidad de los gastos asociados Debe elaborarse un presupuesto Plan de inversión Ofertas de servicios de otros proveedores	Debe evaluar costos reales asociados a la prestación de servicios Ofertas de servicios de otros proveedores Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio Definir si es un servicio esencial	Crear un documento de gestión de accesos. Crear documento de solicitud de accesos	Ofertas de servicios de otros proveedores Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio

	Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio Definir si es un servicio esencial Definir si es un servicio de soporte Evaluación de externalización del servicio Elaboración de un SLA Elaboración de contratos de soporte Elaboración del plan de capacidad	Evaluación de externalización del servicio Elaboración de un SLA Elaboración de contratos de soporte Elaboración del plan de capacidad		
--	--	---	--	--

	Elaborar política de seguridad			
COBIT	La organización debe establecer una política de adquisición de servicios a terceros. Se debe adquirir los servicios de comunicación necesarios para suplir con las necesidades de la empresa. La organización deberá establecer un plan de adquisición de servicios de comunicaciones acorde a las necesidades actuales. Se debe establecer un plan de adquisición de proveedor de comunicación en el cual se establezca el proceso a seguir para realizar la contratación.	Se deben definir estándares en base al nivel de seguridad que requieran las comunicaciones de la organización.	La organización deberá establecer políticas de acuerdo con el nivel de seguridad requerido.	Debe establecerse una política de adquisición de servicios de comunicación en donde se estipulen las condiciones que el proveedor deberá cumplir.

ISO 27000	Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización. Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica, información de la organización.	Hay que gestionar y controlar las redes para proteger la información del sistema y de las aplicaciones. Se debe separar por grupos de servicios de información, usuarios y sistemas de información.	El acceso de los usuarios debe limitarse a la red o a los servicios de red que han sido autorizados a utilizar.	En los contratos de servicios de red se deben identificar e incluir mecanismos de seguridad, niveles de servicio y requisitos para todos los servicios de red, ya sea que los servicios sean prestados por la misma organización o por un tercero.
-----------	---	--	--	---

A.2.3 Instrumento 3

Unidad de análisis:	Servicios TI.			
Variable:	Administración.			
Técnica:	Análisis de contenido.			
Instrumento:	Cuadro resumen.			
Objetivo:	El instrumento pretende consolidar las políticas de administración de TI establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.			
Cuadro resumen				
Metodología / administración	Cuentas de correo electrónico	Asignación de equipo informático	Priorización de recursos	Administración de equipos
ITIL	Crear documento para la petición de servicio (RFC, Request For Change)		Gestión de incidencias y sus clasificaciones de urgencia e impacto de los servicios.	Consola de monitorización de equipos y servicios Respaldo y restauración de archivos Gestión de impresión y salidas para la recopilación de documentos impresos u otros entregables electrónicos

					Actividades de rendimiento o mantenimiento en Gestión de las instalaciones
COBIT				La organización deberá priorizar los recursos de TI para satisfacer los requerimientos en un primer momento, así como para su crecimiento a corto y largo plazo.	La organización debe establecer políticas para revisar y autorizar las adquisiciones importantes de hardware, dentro de los límites aprobados por la junta directiva.
ISO 27000	Debe protegerse adecuadamente la información enviada por mensajes electrónicos.	Debe implementarse un procedimiento para el registro y la baja de usuarios para habilitar los derechos de acceso. Debe controlarse la autenticación de la información de autenticación secreta de los usuarios	Debe aplicarse un procedimiento oficial de prestación de acceso de los usuarios para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.	Debe restringirse y supervisarse la asignación y el uso de los derechos de acceso privilegiado. Se debe retirar el derecho de acceso de todos los trabajadores y de terceros a la información y a las instalaciones de tratamiento de la información al finalizar la contratación, el	

		mediante un proceso de gestión formal.		contrato o el acuerdo, o se debe modificar después de un cambio.
--	--	--	--	--

A.2.4 Instrumento 4

Unidad de análisis:	Sistemas informáticos.						
Variable:	Software.						
Técnica:	Análisis de contenido.						
Instrumento:	Cuadro resumen.						
Objetivo:	El instrumento pretende consolidar las políticas de software establecidas en las metodologías ITIL, COBIT y ISO 27001 en un cuadro resumen.						
Cuadro resumen							
Metodología / software	Licenciamiento	Inventario	Respaldos de la información	Usuarios	Desarrollo de software	Adquisición de software	Renovación de software
ITIL	Elaboración de presupuesto Política de control de precios Portafolio de servicios Plan de gestión de la demanda		Plan de seguridad		Evaluación del valor del servicio Inversión necesaria Evaluación de la utilidad Evaluación de la garantía	Debe evaluar costos reales asociados a la prestación de servicios Llevar la contabilidad de los gastos asociados	Debe elaborarse un presupuesto Plan de inversión Definir si es un servicio esencial

Plan de gestión de la capacidad				Documentar los recursos requeridos Evaluación del tipo de proveedor Evaluación de costes Contabilidad de gastos asociados al servicio Evaluación del presupuesto Evaluación de costes variables Verificación de la Política de fijación de precios Especificación de servicios que se ofrecerán	Debe elaborarse un presupuesto Plan de inversión Ofertas de servicios de otros proveedores Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio Definir si es un servicio esencial Definir si es un servicio de soporte Evaluación de externalización del servicio	Definir si es un servicio de soporte Evaluación de externalización del servicio Revisión del SLA Revisión de contratos de soporte Revisión del plan de capacidad Elaborar manual de requisitos de disponibilidad del negocio Evaluación de riesgos contra la continuidad del servicio

								Analizar el rendimiento de la infraestructura Realizar modelos de simulación de capacidad Gestionar la demanda del servicio racionalizando su uso Determinar los requisitos de disponibilidad Monitorizar la disponibilidad del servicio Proposición de mejoras en la infraestructura para aumentar		
--	--	--	--	--	--	--	--	---	--	--

								la disponibilidad Desarrollar un plan de disponibilidad Mantenimiento del servicio en operación y recuperación de este en caso de fallo Realizar diagnósticos periódicos Evaluar la capacidad de los proveedores internos y externos Evaluar el impacto de las políticas de		
--	--	--	--	--	--	--	--	--	--	--

								seguridad en la disponibilidad Establecer política de continuidad Evaluar el impacto por interrupciones del servicio Evaluar los riesgos a los que está expuesta la infraestructura Establecer la estrategia de continuidad Adoptar medidas proactivas de prevención de riesgos			
--	--	--	--	--	--	--	--	--	--	--	--

[illegible]

							planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.	
ISO 27000	Es preciso establecer procedimientos adecuados para asegurar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales en relación con	Se deben identificar los activos e instalaciones asociados con la información y el procesamiento de la información,	La realización de copias de seguridad de la información, el software y las imágenes del sistema se debe realizar y comprobar de forma habitual, según la	Para habilitar los derechos de acceso, debe realizarse un proceso de registro y cancelación de usuarios. Debe aplicarse un procedimiento	En los requisitos relacionados con la seguridad de la información deben incluirse los requisitos de los nuevos sistemas de información o sistemas de	En los requisitos relacionados con la seguridad de la información deben incluirse los requisitos de los nuevos sistemas de información o	En los requisitos relacionados con la seguridad de la información deben incluirse los requisitos de los nuevos sistemas de información o	

los derechos de propiedad intelectual y la utilización de productos informáticos registrados.	y debe diseñarse y mantenerse un inventario de estos activos.	política de copias de seguridad de la organización.	estructurado de concesión de acceso a los usuarios con el fin de asignar o anular los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios. La atribución y utilización de permisos de acceso privilegiado debe ser restringida y regulada. Se debe controlar la	en la mejora de los sistemas de información existentes. Proteger La información que proviene de los servicios de la aplicación, para evitar el riesgo de la transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes.	información existentes. Proteger La información que proviene de los servicios de la aplicación, para evitar el riesgo de la transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes.	en la mejora de los sistemas de información existentes. Proteger La información que proviene de los servicios de la aplicación, para evitar el riesgo de los servicios de la aplicación, para evitar el riesgo de la transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes.
---	---	---	---	---	---	--

				asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal. Los dueños de los recursos han de verificar periódicamente los derechos de acceso de los usuarios. Se debe retirar a todos los empleados y a terceros el permiso de acceso a la			
--	--	--	--	---	--	--	--

				información y a las instalaciones de tratamiento de la información al término de la relación laboral, contrato o acuerdo, o bien adaptarlo después de un cambio.				
--	--	--	--	--	--	--	--	--

A.2.5 Instrumento 5

Unidad De Análisis:	Seguridad			
Variable:	Riesgo			
Técnica:	Análisis de contenido			
Instrumento:	Cuadro resumen			
Objetivo:	El instrumento nos permite medir los controles que están tomando para la seguridad de las empresas			
Cuadro resumen				
Metodología	Actualización Aplicaciones	Protección antivirus y análisis periódico.	Realizar Copias de seguridad	Controles de acceso
ITIL	Evaluar los costes asociados a la prestación del servicio Asesorar al cliente sobre el valor añadido que proporcionan los servicios de TI prestados Elaboración de presupuesto Verificación de SLA			

Evaluación de externalización de servicios Evaluación del plan de capacidad Evaluación del plan de disponibilidad Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios Analizar el impacto a la continuidad del servicio Elaborar el plan de prevención de riesgos Elaborar el plan de gestión de emergencias Elaborar el plan de recuperación Elaboración de RFC para iniciar actualización Elaboración del plan de actualización			
--	--	--	--

Requisitos internos y externos a tener en cuenta Revisar la documentación del cambio a aplicar Comprobar los elementos de configuración Identificar todos los cambios que incluye la actualización Definir las fases y plazos de la ejecución del cambio Asignar los recursos para el cambio Clasifica el tipo de entrega si es mayor, menor o emergencia Elaboración del Comité Asesor del Cambio (CAB) para validar los cambios a implementar Definir al gestor de cambios que sea el responsable del cambio			
--	--	--	--

Evaluar las RFC para su aprobación Planificar la gestión de cambios Convocar a reunión del CAB para cambios menores y aprobación de las RFC Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas Verificar el cumplimiento de las calendarizaciones propuestas Verificar que la asignación de recursos es la adecuada Desarrollo de un ambiente de pruebas que simule el ambiente de producción Plan de marcha atrás (Back-out) para la recuperación ante un fallo			
--	--	--	--

Establecer una política de implementación de nuevas versiones de hardware y software Implementar las nuevas versiones de software y hardware en el entorno de producción después de que la validación y pruebas las haya verificado en un entorno realista Garantizar que el proceso de cambio cumpla con las especificaciones de la RFC Asegurar que todos los cambios se ven correctamente reflejados Implementar un control de versionamiento Elaboración del plan de entrega			
--	--	--	--

	Pruebas del correcto funcionamiento de la versión Pruebas de los manuales de instalación Prueba de los planes de Back-out Pruebas funcionales por los usuarios			
COBIT	Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar,	Se deben establecer procesos con el propósito de minimizar el impacto al negocio debido a vulnerabilidades e incidentes de seguridad de la información, entre lo cual involucra establece un mecanismo de protección contra malware.	Se deben realizar copias de seguridad de datos regulares diariamente. Esa copia de seguridad podrá ser almacenada en un medio físico (por ejemplo, cinta o disco duro externo), o podría ser a una ubicación remota a través de la nube (es decir, Internet). Si una empresa realiza una copia de seguridad por un medio físico, se recomienda que las copias de seguridad se realicen en diferentes medios a	Se deben realizar controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas estén restringidos a usuarios autorizados, con el fin de salvaguardar la información contra uso no autorizado, divulgación,

	evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.		fin de garantizar la disponibilidad e integridad de dicha copia de seguridad.	modificación, daño o pérdida.
ISO27000	Los cambios en todos los sistemas durante el ciclo de vida del desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. Cuando se producen cambios en las plataformas operativas, hay que revisar y probar las aplicaciones críticas para la empresa a fin de asegurarse de que no afecten negativamente a las	Los controles de detección, prevención y recuperación se deben implementar para proteger contra el software malicioso, combinado con una adecuada concienciación de los usuarios.	Se debe hacer una copia de seguridad de la información, el software y las imágenes del sistema y se deben probar de forma periódica de conformidad con la política de copias de seguridad.	Hay que establecer, documentar y analizar una política de control de acceso que se base en los requisitos de seguridad de la información y de las actividades de la empresa. Los usuarios deben recibir sólo acceso a la red y servicios de

operaciones o a la seguridad de la organización. Se debe desaconsejar la realización de modificaciones a los paquetes de software, limitándolas a cambios necesarios, y todos los cambios deben ser estrictamente controlados. En cualquier iniciativa de implementación de sistemas de información se deberán establecer, documentar, mantener y poner en práctica principios para la ingeniería de sistemas seguros. La Organización debe controlar y supervisar las actividades de desarrollo de los sistemas subcontratados.		red específicamente autorizados. Para que sea posible la asignación de derechos de acceso, es necesario que se establezca un procedimiento formal de creación y cancelación de usuarios. Se debe poner en práctica un procedimiento formal para asignar o revocar los derechos de acceso de todos los tipos de usuarios a todos los sistemas y servicios. La asignación y el uso de los privilegios de los
---	--	---

Durante el desarrollo del sistema se deben realizar pruebas de la funcionalidad de seguridad del mismo. Deben elaborarse programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.		derechos de acceso deben ser restringidos y controlados. Se debe realizar la Administración de la información de autenticación secreta de los usuarios Se debe controlar la asignación de la información de autenticación secreta a través de un proceso de gestión formal. Cada cierto tiempo, los gestores de recursos deben revisar los derechos de acceso de los usuarios.
---	--	--

					En caso de terminación de la relación laboral, contrato o acuerdo, o en caso de que se produzca un traspaso, deberán revocarse los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de la información.
--	--	--	--	--	---

A.2.6 Instrumento 6

Unidad De Análisis:	Requisitos indispensables de cada metodología
Variable:	Requisitos
Técnica:	Análisis de contenido
Instrumento:	Cuadro resumen
Objetivo:	

El instrumento nos permite tomar en consideración los requisitos para cada normativa

Cuadro resumen		
	ITIL	COBIT
Requisitos	• Debe evaluar costos reales asociados a la prestación de servicios • Llevar la contabilidad de los gastos asociados • Debe elaborarse un presupuesto • Plan de inversión • Ofertas de servicios de otros proveedores	• Se debe establecer un plan de adquisiciones de tecnología que se alinee con el plan de infraestructura tecnológica. • Se deben contar con procesos para actualizar la infraestructura tecnológica. • Se debe contar con un manual el cual establezca el uso del hardware por los usuarios.
		• Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización. • Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de

	• Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio • Definir si es un servicio esencial • Definir si es un servicio de soporte • Evaluación de externalización del servicio • Elaboración de un SLA • Elaboración de contratos de soporte • Elaboración del plan de capacidad • Elaborar manual de requisitos de disponibilidad del negocio • Evaluación de riesgos contra la continuidad del servicio • Plan de recuperación • Elaborar política de seguridad • Debe elaborarse un presupuesto • Plan de inversión • Definir si es un servicio esencial • Definir si es un servicio de soporte	• Determinar la dirección tecnológica, mediante la creación de un plan de infraestructura tecnológica el cual considere el número de equipos de TI con los que cuente la empresa. • Evaluar el desempeño del hardware actual, a fin de establecer un plan de renovación de equipos. • Establecer un plan de adquisición de servicios de comunicaciones acorde a las necesidades actuales. • Definir estándares en base al nivel de seguridad que requieran las comunicaciones de la organización. • Establecer políticas de acuerdo con el nivel de seguridad requerido.	infraestructura tecnológica, información de la organización. • Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica, información de la organización. • Los requisitos de seguridad de la información deben ser definidos y consensuados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica, información de la organización. • Los activos e instalaciones asociados con la información y el procesamiento de la información han de identificarse, y se ha de diseñar y mantener un inventario de dichos activos. • Los bienes inventariados deben asignarse a un propietario.
--	--	--	---

• Evaluación de externalización del servicio • Revisión del SLA • Revisión de contratos de soporte • Revisión del plan de capacidad • Elaborar manual de requisitos de disponibilidad del negocio • Evaluación de riesgos contra la continuidad del servicio • Evaluación de riesgos contra la continuidad del servicio • Plan de recuperación • Elaborar política de seguridad • Monitorear los recursos mediante los SLA • Monitorear la disponibilidad evaluando el tiempo esperado versus tiempo de interrupción • Elaborar política de seguridad • Elaborar política de seguridad • Debe elaborarse un presupuesto • Definir si es un servicio esencial	• Establecerse una política de adquisición de servicios de comunicación en donde se estipulen las condiciones que el proveedor deberá cumplir. • Priorizar los recursos de TI para satisfacer los requerimientos en un primer momento, así como para su crecimiento a corto y largo plazo. • Establecer políticas para revisar y autorizar las adquisiciones importantes de hardware, dentro de los límites aprobados por la junta directiva. • Suministrar recursos TI de software. • Definir un plan estratégico de TIC, el cual logre un balance óptimo entre cubrir las necesidades del negocio y oportunidades tecnológicas.	• Se deben aplicar, documentarse y ejecutarse normas para la utilización aceptable de la información y los bienes relacionados con las instalaciones de tratamiento de la información. • Todos los empleados y los usuarios internos y externos deberán devolver todos los activos de la organización en su poder al término de su empleo, contrato o acuerdo. • Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica. • El equipo de mantenimiento debe ser adecuadamente atendido para asegurar una disponibilidad e integridad continuas. • Los equipos no pueden ser retirados de su lugar sin autorización previa. • Se debe acordar y documentar los requisitos de seguridad de la información
--	---	---

	• Definir si es un servicio de soporte • Evaluación de externalización del servicio • Revisión del SLA • Revisión de contratos de soporte • Evaluación de riesgos contra la continuidad del servicio • Plan de recuperación • Elaborar política de seguridad • Debe evaluar costos reales asociados a la prestación de servicios • Llevar la contabilidad de los gastos asociados • Debe elaborarse un presupuesto • Plan de inversión • Ofertas de servicios de otros proveedores • Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio • Definir si es un servicio esencial	• Definir procesos de respaldo y recuperación de sus sistemas, los cuales garanticen mantener las operaciones principales disponibles. • Establecer procesos para la definición de requerimientos, planeación, desarrollo, pruebas y puesta en marcha de un nuevo software. • Establecer un proceso el cual permita la adquisición de un software previo a un estudio donde se establezcan los requerimientos, y en base a las políticas de proveedores de la empresa. • Establecer un proceso el cual permita evaluar el desempeño actual del software en la organización y en base al grado de cumplimiento que estos den al negocio, se deberá establecer	para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización. • Se deben establecer y acordar todos los requisitos en relación con la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar elementos de infraestructura tecnológica, información de la organización. • Hay que gestionar y controlar las redes para proteger la información del sistema y de las aplicaciones. • Se debe separar por grupos de servicios de información, usuarios y sistemas de información. • El acceso de los usuarios debe limitarse a la red o a los servicios de red que han sido autorizados a utilizar. • En los contratos de servicios de red se deben identificar e incluir mecanismos de seguridad, niveles de servicio y requisitos para todos los servicios de red, ya sea que
--	--	---	--

• Definir si es un servicio de soporte • Evaluación de externalización del servicio • Elaboración de un SLA • Elaboración de contratos de soporte • Elaboración del plan de capacidad • Elaborar manual de requisitos de disponibilidad del negocio • Evaluación de riesgos contra la continuidad del servicio • Plan de recuperación • Elaborar política de seguridad • Debe evaluar costos reales asociados a la prestación de servicios • Ofertas de servicios de otros proveedores • Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio • Definir si es un servicio esencial	un proceso para la actualización del software a una versión más reciente o su cambio por otra solución. • Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente. • Realizar copias de seguridad de datos regulares diariamente. Esa copia de seguridad podrá ser almacenada en un medio físico (por ejemplo, cinta o disco duro externo), o podría ser a una ubicación remota a través de la nube (es decir, Internet). • Controles de acceso lógico que aseguren que el acceso a	los servicios sean prestados por la misma organización o por un tercero. • Debe protegerse adecuadamente la información enviada por mensajes electrónicos. • Debe implementarse un procedimiento para el registro y la baja de usuarios para habilitar los derechos de acceso. • Debe controlarse la autenticación de la información de autenticación secreta de los usuarios mediante un proceso de gestión formal. • Debe aplicarse un procedimiento oficial de prestación de acceso de los usuarios para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios. • Debe restringirse y supervisarse la asignación y el uso de los derechos de acceso privilegiado. • Se debe retirar el derecho de acceso de todos los trabajadores y de terceros a la información y a las instalaciones de
---	--	---

	• Evaluación de externalización del servicio • Elaboración de un SLA • Elaboración de contratos de soporte • Elaboración del plan de capacidad • Crear un documento de gestión de accesos. • Crear documento de solicitud de accesos • Ofertas de servicios de otros proveedores • Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio • Crear documento para la petición de servicio (RFC, Request For Change) • Gestión de incidencias y sus clasificaciones de urgencia e impacto de los servicios.	sistemas, datos y programas estén restringidos a usuarios autorizados. • Se deben establecer procesos para desarrollar y transmitir la documentación de cada uno de los procesos de la organización. • Se deben establecer procesos para la evaluación, asignación de prioridad y autorizaciones de cambio. • Se deben establecer una metodología de pruebas sobre los nuevos desarrollos. • Se debe establecer un proceso de aprobación de las pruebas en base al cumplimiento de las necesidades del negocio. • Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la	tratamiento de la información al finalizar la contratación, el contrato o el acuerdo, o se debe modificar después de un cambio. • Es preciso establecer procedimientos adecuados para asegurar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales en relación con los derechos de propiedad intelectual y la utilización de productos informáticos registrados. • Se deben identificar los activos e instalaciones asociados con la información y el procesamiento de la información, y debe diseñarse y mantenerse un inventario de estos activos. • La realización de copias de seguridad de la información, el software y las imágenes del sistema se debe realizar y comprobar de forma habitual, según la política de copias de seguridad de la organización.
--	---	--	---

• Consola de monitorización de equipos y servicios • Respaldo y restauración de archivos • Gestión de impresión y salidas para la recopilación de documentos impresos u otros entregables electrónicos • Actividades de rendimiento o mantenimiento en beneficio de los equipos • Gestión de las instalaciones • Elaboración de presupuesto • Política de control de precios • Portafolio de servicios • Plan de gestión de la demanda • Plan de gestión de la capacidad • Plan de seguridad • Evaluación del valor del servicio • Inversión necesaria • Evaluación de la utilidad • Evaluación de la garantía	• Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información en toda la empresa. • Crear y mantener un inventario de información que incluya un listado de los propietarios, custodios y clasificaciones. • Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias. • Llevar revisiones periódicas de las habilidades y competencias del recurso humano interno y externo. • Desarrollar planes de mejoras de desempeño basado en resultados de procesos de evaluación.	• Para habilitar los derechos de acceso, debe realizarse un proceso de registro y cancelación de usuarios. • Debe aplicarse un procedimiento estructurado de concesión de acceso a los usuarios con el fin de asignar o anular los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios. • La atribución y utilización de permisos de acceso privilegiado debe ser restringida y regulada. • Se debe controlar la asignación de la información de autenticación • secreta de usuarios mediante un proceso de gestión formal. • Los dueños de los recursos han de verificar periódicamente los derechos de acceso de los usuarios. • Se debe retirar a todos los empleados y a terceros el permiso de acceso a la información y a las instalaciones de tratamiento de la información al término de
--	---	--

• Documentar los recursos requeridos • Evaluación del tipo de proveedor • Evaluación de costes • Contabilidad de gastos asociados al servicio • Evaluación del presupuesto • Evaluación de costes variables • Verificación de la Política de fijación de precios • Especificación de servicios que se ofrecerán • Verificación de la gestión del portafolio de servicios • Diseño de paquetes de servicio • Evaluación de la demanda • Evaluación de la externalización del servicio • Diseño de evaluación de la arquitectura del servicio • Elaboración de métricas de monitorización	• Crear y mantener un inventario de recursos humanos de negocio y TI. • Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios de TI nuevos o rediseñados. • Revisar acuerdos y políticas de los contratos. • Establecer un sistema de gestión de la calidad. • Definir y gestionar estándares, procesos y prácticas de calidad. • Supervisar y hacer controles y revisiones de la calidad. • Realizar un análisis de los riesgos potenciales y su impacto en el negocio. • Realizar escenarios de riesgos de TI.	la relación laboral, contrato o acuerdo, o bien adaptarlo después de un cambio. • En los requisitos relacionados con la seguridad de la información deben incluirse los requisitos de los nuevos sistemas de información o en la mejora de los sistemas de información existentes. • Proteger La información que proviene de los servicios de la aplicación, para evitar el riesgo de la • transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes. • En los requisitos relacionados con la seguridad de la información deben incluirse los requisitos de los nuevos sistemas de información o en la mejora de los sistemas de información existentes. • Proteger La información que proviene de los servicios de la aplicación, para evitar el riesgo de la
--	--	--

	• Elaboración de los SLA • Analizar el rendimiento de la infraestructura • Realizar modelos de simulación de capacidad • Gestionar la demanda del servicio racionalizando su uso • Determinar los requisitos de disponibilidad • Monitorizar la disponibilidad del servicio • Proposición de mejoras en la infraestructura para aumentar la disponibilidad • Desarrollar un plan de disponibilidad • Mantenimiento del servicio en operación y recuperación de este en caso de fallo • Realizar diagnósticos periódicos • Evaluar la capacidad de los proveedores internos y externos	• Definir un portafolio de acciones a seguir para la gestión de riesgos. • Establecer y mantener un SGSI. • Definir y gestionar un plan de tratamiento de riesgo de la seguridad de la información. • Definir y mantener los requerimientos técnicos y funcionales del negocio. • Realizar estudios de viabilidad para proponer soluciones alternativas. • Identificar y registrar los activos actuales de TI. • Gestionar el ciclo de vida de los activos de TI. • Mantener un registro de todas las licencias de software adquiridos y acuerdos de licencias asociados.	• transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes. • En los requisitos relacionados con la seguridad de la información deben incluirse los requisitos de los nuevos sistemas de información o en la mejora de los sistemas de información existentes. • Proteger La información que proviene de los servicios de la aplicación, para evitar el riesgo de la • transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes. • Los cambios en todos los sistemas durante el ciclo de vida del desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. • Cuando se producen cambios en las plataformas operativas, hay que revisar y probar las aplicaciones críticas para la empresa a fin de asegurarse de que no
--	---	--	---

	• Evaluar el impacto de las políticas de seguridad en la disponibilidad • Establecer política de continuidad • Evaluar el impacto por interrupciones del servicio • Evaluar los riesgos a los que está expuesta la infraestructura • Establecer la estrategia de continuidad • Adoptar medidas proactivas de prevención de riesgos • Desarrollar plan de contingencia • Política de seguridad • Debe evaluar costos reales asociados a la prestación de servicios • Llevar la contabilidad de los gastos asociados • Debe elaborarse un presupuesto • Plan de inversión • Ofertas de servicios de otros proveedores	• Llevar a cabo auditorías para identificar a todas las copias de software instalado con licencia. • Establecer y mantener una política de seguridad para las conexiones. • Cifrar la información en tránsito de acuerdo a su clasificación. • Aplicar protocolos de seguridad aprobados a las conexiones de red. • Configurar sistemas operativos de forma segura. • Configurar los equipamientos de red en forma segura. • Realizar pruebas periódicas de la seguridad del sistema. • Implementar mecanismos de bloqueo a dispositivos. • Cifrar información de acuerdo con su clasificación.	afecten negativamente a las operaciones o a la seguridad de la organización. • Se debe desaconsejar la realización de modificaciones a los paquetes de software, limitándolas a cambios necesarios, y todos los cambios deben ser estrictamente controlados. • En cualquier iniciativa de implementación de sistemas de información se deberán establecer, documentar, mantener y poner en práctica principios para la ingeniería de sistemas seguros. • La Organización debe controlar y supervisar las actividades de desarrollo de los sistemas subcontratados. • Durante el desarrollo del sistema se deben realizar pruebas de la funcionalidad de seguridad del mismo. • Deben elaborarse programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.
--	---	---	---

• Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio • Definir si es un servicio esencial • Definir si es un servicio de soporte • Evaluación de externalización del servicio • Elaboración de un SLA • Elaboración de contratos de soporte • Elaboración del plan de capacidad • Elaborar manual de requisitos de disponibilidad del negocio • Evaluación de riesgos contra la continuidad del servicio • Plan de recuperación • Elaborar política de seguridad • Debe elaborarse un presupuesto • Plan de inversión • Definir si es un servicio esencial • Definir si es un servicio de soporte	• Gestionar el acceso y control remoto. • Proveer protección física a los dispositivos de usuario final. • Deshacerse de los dispositivos de usuario final de forma segura. • Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basado en roles de puestos predefinidos. • Revisar periódicamente la definición de los controles de acceso. • Gestión de errores y excepciones. • Definir un esquema de clasificación para identificar todos los elementos de coste relacionados con TI.	• Los controles de detección, prevención y recuperación se deben implementar para proteger contra el software malicioso, combinado con una adecuada concienciación de los usuarios. • Se debe hacer una copia de seguridad de la información, el software y las imágenes del sistema y se deben probar de forma periódica de conformidad con la política de copias de seguridad. • Hay que establecer, documentar y analizar una política de control de acceso que se base en los requisitos de seguridad de la información y de las actividades de la empresa. • Los usuarios deben recibir sólo acceso a la red y servicios de red específicamente autorizados. • Para que sea posible la asignación de derechos de acceso, es necesario que se establezca un procedimiento formal de creación y cancelación de usuarios.
--	--	---

• Evaluación de externalización del servicio • Revisión del SLA • Revisión de contratos de soporte • Revisión del plan de capacidad • Elaborar manual de requisitos de disponibilidad del negocio • Evaluación de riesgos contra la continuidad del servicio • Evaluación de riesgos contra la continuidad del servicio • Plan de recuperación • Elaborar política de seguridad • Evaluar los costes asociados a la prestación del servicio • Asesorar al cliente sobre el valor añadido que proporcionan los servicios de TI prestados • Elaboración de presupuesto • Verificación de SLA • Evaluación de externalización de servicios	• Utilizar la información financiera y de cartera para proporcionar datos de entrada a casos de negocio para nuevas inversiones en activos y servicios de TI. • Establecer un órgano de toma de decisiones para priorizar recursos de TI y del negocio. • Crear un presupuesto formal de TI, el cual incluya todos los costos relacionados a este rubro y el cual vaya alineado con la situación actual del negocio. • Identificar todos los procesos de negocio internos o subcontratados que son críticos para las operaciones de la empresa o necesarios para cumplir las obligaciones legales y/o contractuales.	• Se debe poner en práctica un procedimiento formal para asignar o revocar los derechos de acceso de todos los tipos de usuarios a todos los sistemas y servicios. • La asignación y el uso de los privilegios de los derechos de acceso deben ser restringidos y controlados. • Se debe realizar la Administración de la información de autenticación secreta de los usuarios • Se debe controlar la asignación de la información de autenticación secreta a través de un proceso de gestión formal. • Cada cierto tiempo, los gestores de recursos deben revisar los derechos de acceso de los usuarios. • En caso de terminación de la relación laboral, contrato o acuerdo, o en caso de que se produzca un traspaso, deberán revocarse los derechos de acceso de todos los empleados y usuarios externos a la
--	---	---

• Evaluación del plan de capacidad • Evaluación del plan de disponibilidad • Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios • Analizar el impacto a la continuidad del servicio • Elaborar el plan de prevención de riesgos • Elaborar el plan de gestión de emergencias • Elaborar el plan de recuperación • Elaboración de RFC para iniciar actualización • Elaboración del plan de actualización • Requisitos internos y externos a tener en cuenta • Revisar la documentación del cambio a aplicar	• Identificar los procesos de soporte al negocio esenciales y servicios de TI. • Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes • Definir las acciones y comunicaciones en respuesta a incidentes que deben ser realizados en un evento de disrupción.	información y a las instalaciones de procesamiento de la información.
--	--	--

- Comprobar los elementos de configuración
- Identificar todos los cambios que incluye la actualización
- Definir las fases y plazos de la ejecución del cambio
- Asignar los recursos para el cambio
- Clasifica el tipo de entrega si es mayor, menor o emergencia
- Elaboración del Comité Asesor del Cambio (CAB) para validar los cambios a implementar
- Definir al gestor de cambios que sea el responsable del cambio
- Evaluar las RFC para su aprobación
- Planificar la gestión de cambios
- Convocar a reunión del CAB para cambios menores y aprobación de las RFC

- Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas
- Verificar el cumplimiento de las calendarizaciones propuestas
- Verificar que la asignación de recursos es la adecuada
- Desarrollo de un ambiente de pruebas que simule el ambiente de producción
- Plan de marcha atrás (Back-out) para la recuperación ante un fallo
- Establecer una política de implementación de nuevas versiones de hardware y software
- Implementar las nuevas versiones de software y hardware en el entorno de producción después de que la validación y pruebas las haya verificado en un entorno realista

- Garantizar que el proceso de cambio cumpla con las especificaciones de la RFC
- Asegurar que todos los cambios se ven correctamente reflejados
- Implementar un control de versionamiento
- Elaboración del plan de entrega
- Pruebas del correcto funcionamiento de la versión
- Pruebas de los manuales de instalación
- Prueba de los planes de Back-out
- Pruebas funcionales por los usuarios

A.2.7 Instrumento 7

Unidad de análisis:	Criterios de clasificación de micro y pequeña empresa		
Variable:	Estructura organizativa		
Técnica:	Análisis de contenido		
Instrumento:	Cuadro resumen		
Objetivo:	El instrumento utilizado como cuadro resumen es para conocer parte del carácter de cualquier tipo de empresa. Por lo tanto, la importancia de la estructura organizativa nos ayuda a conocer como base de la propia cultura organizativa.		
	Cuadro resumen		
	Número de empleados	Ubicación geográfica	Autoridad central o descentralizada
Microempresa	Hasta 10	29.47% en el área metropolitana de San Salvador.	Autoridad central
		36.53% en servicios.	
		11.54% en industria	
		23.80% en la zona occidental.	
		19.47% en la zona oriental.	

		19.18% en la zona central.		
		8.08% en la zona paracentral.		
Pequeña Empresa	11 a 50	42.29% en el área metropolitana de San Salvador.	63.64% en comercio. 27.33% en servicio.	Autoridad central o descentralizada
		22.33% en la zona occidental.	7.82% en industria.	
		22.06% en la zona oriental.		
		9.89% en la zona central.		
		3.48% en la zona paracentral.		

Fuente: CONAMYPE (3)

A.2.8 Instrumento 8

Unidad De Análisis:	Criterios de clasificación de micro y pequeña empresa		
Variable:	Financiero		
Técnica:	Análisis de contenido		
Instrumento:	Cuadro resumen		
Objetivo:	Determinar la inversión destinada al área de tecnología		
	Cuadro resumen		
		Capital de la Empresa	Presupuesto TI
	Microempresa	Hasta 482 salarios mínimos.	\$590.00 que incluye costo de internet (\$30 aprox.), licencias de office 365 (\$60 aprox.) y capacitación (\$500 aprox.)
	Pequeña Empresa	Mayores a 482 hasta 4817 salarios mínimos.	\$590.00 que incluye costo de internet (\$30 aprox.), licencias de office 365 (\$60 aprox.) y capacitación (\$500 aprox.)

Fuente: CONAMYPE (3)

A.2.9 Instrumento 9

Para llevar a cabo la entrevista se realizó una selección de 10 profesionales en el ámbito de las TIC, obteniendo los siguientes resultados:

1. ¿Cuántos años de experiencia tiene en el ámbito informático?

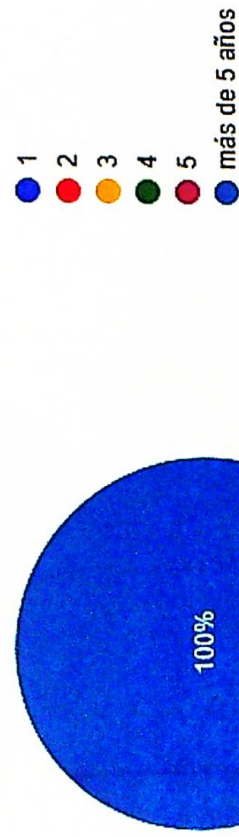


Figura 4. Resultados obtenidos de la pregunta #1

Un 100% de los entrevistados cuentan con más de 5 años de experiencia en el sector.

2. ¿Ha implementado en su trabajo u otros lugares alguna metodología de TIC, tales como COBIT, ITIL o ISO 27001?

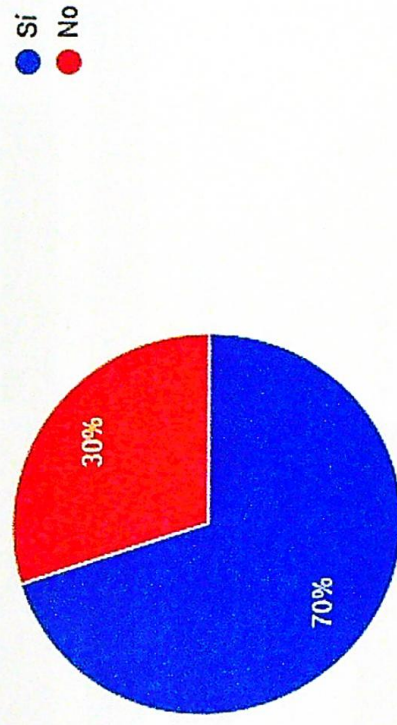


Figura 5. Resultados obtenidos de la pregunta #2

El 70% indica que han implementado metodologías tales como ITIL, COBIT o ISO 27001.

3. ¿Qué metodologías ha implementado?

Las áreas principales que se indican como estratégicas son la gestión de servicios de TIC y la seguridad de la información, colocando a ITIL y COBIT 5 como las mejores metodologías orientadas a la estrategia propia de los servicios y su alineación con los objetivos del negocio. Por otra parte, la seguridad, a pesar de contar con muchas derivaciones enfocadas a la diversidad de las TIC, ha sido muy factible y con resultados positivos la adopción total o parcial de la norma ISO 27001.

4. ¿Cuáles han sido los motivos por los que ha optado por implementarlas?



Figura 6. Resultados obtenidos de la pregunta #4

La motivación principal para implementar estas metodologías, con un 85.7%, es la mejora en los procesos de negocio; seguido con un 57.1% como políticas de empresa.

5. ¿La implementación ha sido apoyada por la alta gerencia, o se ha llevado a cabo por iniciativa propia?

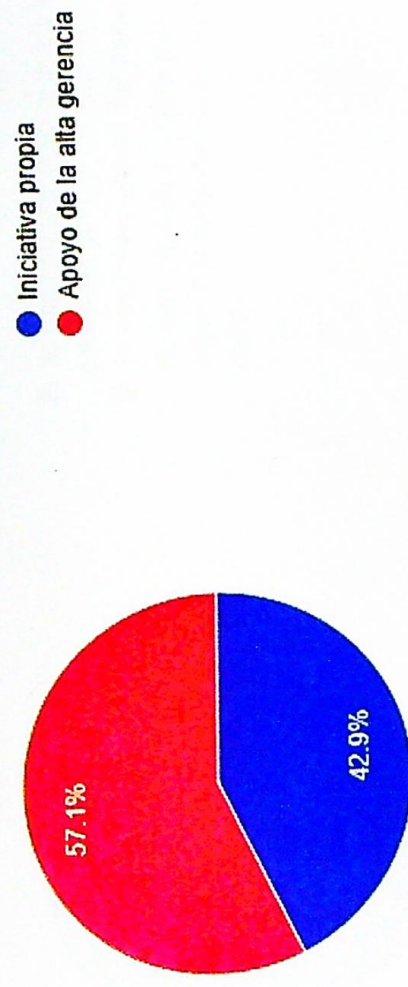


Figura 7. Resultados obtenidos de la pregunta #5

En un margen bastante corto, la implementación por iniciativa propia se lleva a cabo en un 42.9%, seguido de un 57.1% de apoyo por la alta gerencia.

6. ¿Ha tomado como referencia algunas partes de las metodologías considerándolas buenas prácticas, o todas se han llevado a cabo con la finalidad de una implementación completa?

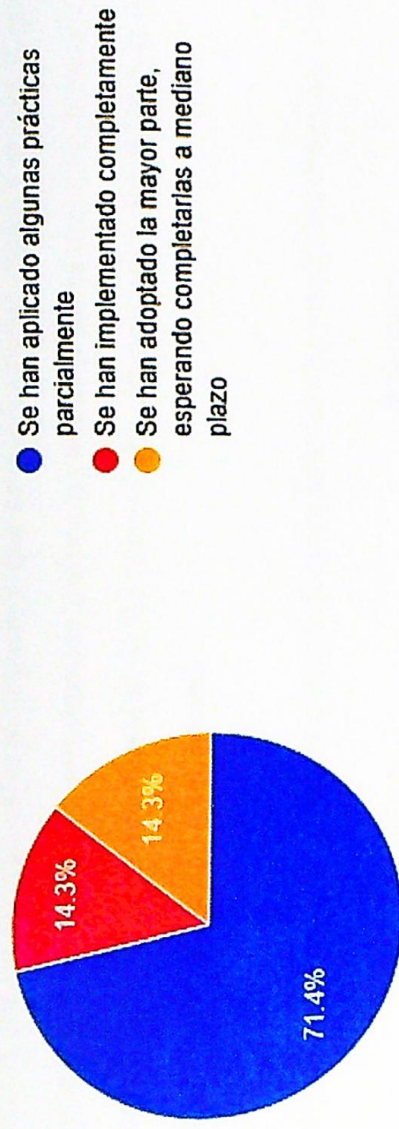


Figura 8. Resultados obtenidos de la pregunta #6

Este indicador nos muestra que en un 71.4% se toman algunas partes para ser aplicadas, enfocadas en las necesidades primarias que se tienen y por términos de recursos que pueden sobrepasar lo ya presupuestado por la empresa.

7. En base a su experiencia ¿Cuál o cuáles considera que son las áreas principales a las que se deben aplicar metodologías TIC?

La seguridad de la información es una de las áreas de mayor interés donde se enfocan los recursos empresariales para identificar y mitigar riesgos que atenten contra la competitividad y el desarrollo de los negocios, esto no solo orientado a herramientas administrativas (Antivirus, anti spam, firewalls, etc.), también abarcando decisiones estratégicas que deben cumplir con requisitos mínimos de seguridad, contratos de servicios, gestión de proveedores y cualquier actividad que abre la oportunidad de compartir información del negocio.

9. ¿Qué otras metodologías conocen?

Otra área importante que se indica es la administración de proyectos TIC que se puede apoyar de PMBOK (Project Management Book Of Knowledge) dado a su amplitud y nivel de especificación de la información propia del proyecto, permitiendo principalmente establecer los lineamientos a los que debe apegarse el proyecto y cada requerimiento a cumplir. A parte de las metodologías en análisis, las orientas a la administración de proyectos informáticos son las más reconocidas. Se mencionan los principios indicados por COSO (Commite Of Sponsoring of the threadway) orientadas a la gestión de riesgos, controles internos orientados a las TIC para garantizar que estas cumplen los objetivos y que no son utilizadas para actividades ilegales. Entre otras se menciona a Val IT como apoyo estratégico para las inversiones de TIC que aumenten el valor de negocio, y, por último, Risk IT, que ayuda a evaluar los riesgos de no aprovechar los beneficios que las TIC ofrecen.

10. Para el caso de micro y pequeña empresa ¿Sería posible implementar parte de las buenas prácticas que las metodologías ofrecen?

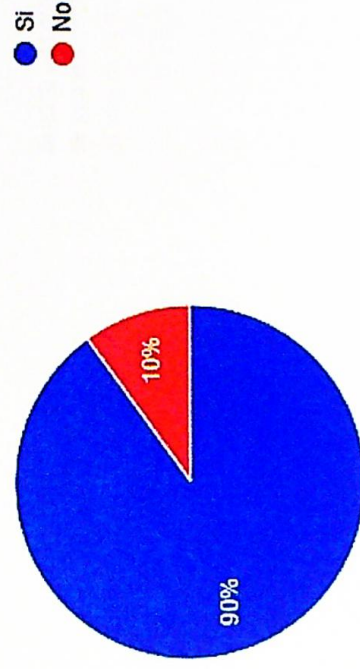


Figura 10. Resultados obtenidos de la pregunta #10

Un 90% coincide con la oportunidad de las micro y pequeñas empresas de implementar parte de las buenas prácticas que las metodologías ofrecen.

11. ¿Considera que hay buenas prácticas de estas metodologías que no requieren un conocimiento especializado de tecnologías de información?

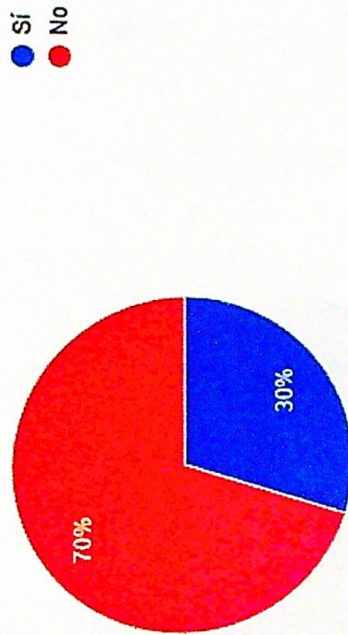


Figura 11. Resultados obtenidos de la pregunta #11

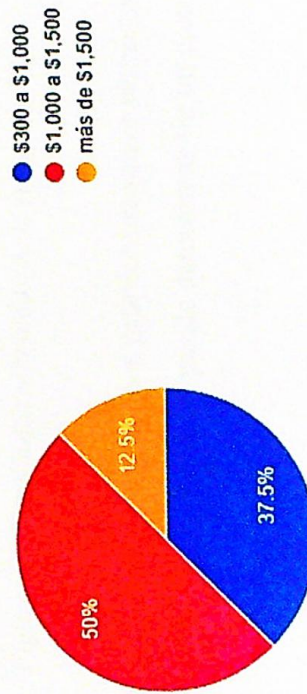


Figura 12. Resultados obtenidos de la pregunta #12

La necesidad de un especialista en TIC se ve reflejada con un 70% de los entrevistados que indican que su costo puede rondar entre los \$300.00 a \$1,500.00 (valor mensual). Se abre la posibilidad de que este costo pudiera expresarse en términos de consultoría que podría rondar un cuarto de los valores expresados anteriormente, es decir, \$75.00 a \$375.00 mensualmente.

12. ¿Considera usted que estas metodologías tienen prácticas que no requieren un costo a quien lo implementa, más que únicamente el esfuerzo de llevarla a cabo?

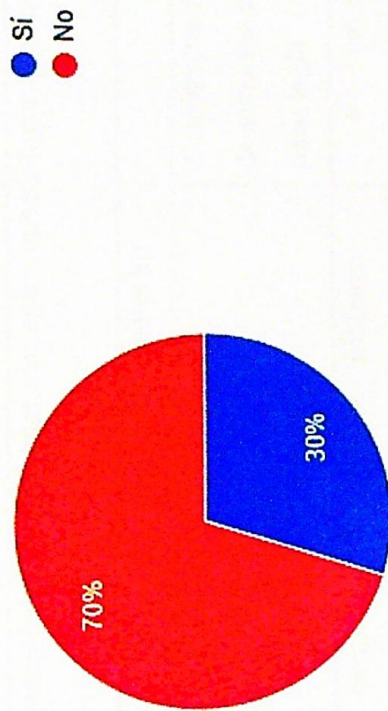


Figura 13. Resultados obtenidos de la pregunta #12

El 70% indica que cualquier parte de implementación de buenas prácticas requiere un costo mínimo, dado que la amplitud de servicios TIC y el análisis de lo que se ajusta al negocio no se puede determinar sin un conocimiento del área.

A.2.10 Instrumento 10

Unidad de análisis:	Estado del arte					
Variable:	Guía de criterios					
Técnica:	Análisis de contenido					
Instrumento:	Cuadro de clasificación					
Objetivo:	Clasificar las buenas prácticas encontradas como obligatorias en las metodologías para una mayor comprensión y segmentación de áreas de aplicación.					
Guía de criterios						
Metodología	Administración de hardware	Administración de software	Seguridad	Administración de servicios de tecnología	Recursos humanos	Gestión del conocimiento
ITIL	Gestión de incidencias y sus clasificaciones de urgencia e impacto de los servicios.	Gestión de incidencias y sus clasificaciones de urgencia e impacto de los servicios.	- Elaborar política de seguridad - Evaluación de riesgos contra la continuidad del servicio	- Plan de inversión - Debe evaluar costos reales asociados a la prestación	Crear un documento de gestión de accesos.	- Monitorear los recursos mediante los SLA - Monitorear la disponibilidad evaluando el tiempo

servicios.		• Respaldo y restauración de archivos • Gestionar la demanda del servicio racionalizando su uso • Mantenimiento del servicio en operación y recuperación de este en caso de fallo • Realizar diagnósticos periódicos • Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios	• Plan de recuperación • Respaldo y restauración de archivos • Elaborar Plan de seguridad • Adoptar medidas proactivas de prevención de riesgos • Desarrollar plan de contingencia • Elaborar el plan de gestión de emergencias	de servicios • Llevar la contabilidad de los gastos asociados • Política de control de precios • Ofertas de servicios de otros proveedores • Previsión de costes directos e indirectos de la creación y	esperado versus tiempo de interrupción • Consola de monitorización de equipos y servicios • Documentar los recursos requeridos • Monitorizar la disponibilidad del servicio • Evaluación de la demanda • Evaluación de la utilidad
------------	--	---	--	--	--

	beneficio de los equipos • Gestión de las instalaciones • Analizar el rendimiento de la infraestructura • Gestionar la demanda del servicio racionalizando su uso • Proposición de mejoras en la infraestructura para aumentar la disponibilidad	• Elaboración de RFC para iniciar actualización • Elaboración del plan de actualización • Revisar la documentación del cambio a aplicar • Comprobar los elementos de configuración • Identificar todos los cambios que incluye la actualización • Definir las fases y plazos de la ejecución del cambio	• Elaborar el plan de recuperación	mantenimiento de cada servicio • Realizar modelos de simulación de capacidad • Elaboración de métricas de monitorización • Diseño de evaluación de la arquitectura del servicio	• Evaluación de la garantía • Evaluación de externalización del servicio • Evaluación de Inversión necesaria • Evaluación del valor del servicio • Evaluar el impacto de las políticas de seguridad en la disponibilidad • Evaluar el impacto por
--	--	--	--	--	--

	• Mantener el nivel de servicio en operación y recuperación de este en caso de fallo • Realizar diagnósticos periódicos • Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios • Elaboración de RFC para iniciar actualización	• Asignar los recursos para el cambio • Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas • Desarrollo de un ambiente de pruebas que simule el ambiente de producción • Plan de marcha atrás (Back-out) para la recuperación ante un fallo		• Desarrollar un plan de disponibilidad • Diseño de paquetes de servicio • Asesorar al cliente sobre el valor añadido que proporcionan los servicios de TI prestados • Definir si es un	interrupciones del servicio • Evaluar los riesgos a los que está expuesta la infraestructura • Revisión del SLA • Revisión de contratos de soporte • Revisión del plan de capacidad • Analizar el impacto a la continuidad del servicio
--	---	--	--	--	--

	• Elaboración del plan de actualización • Revisar la documentación del cambio a aplicar • Comprobar los elementos de configuración • Identificar todos los cambios que incluye la actualización • Definir las fases y	• Implementar las nuevas versiones de software y hardware en el entorno de producción después de que la validación y pruebas las haya verificado en un entorno realista • Garantizar que el proceso de cambio cumpla con las especificaciones de la RFC • Asegurar que todos los cambios se ven correctamente reflejados		servicio esencial • Requisitos internos y externos a tener en cuenta • Establecer la estrategia de continuidad • Establecer política de continuidad • Evaluar la capacidad de los proveedor	
--	---	--	--	---	--

	plazos de la ejecución del cambio	• Asignar los recursos para el cambio • Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas • Desarrollo de un ambiente de pruebas que	• Implementar un control de versionamiento • Pruebas del correcto funcionamiento de la versión • Pruebas de los manuales de instalación • Prueba de los planes de Back-out • Pruebas funcionales por los usuarios		es internos y externos • Definir si es un servicio de soporte • Clasifica el tipo de entrega si es mayor, menor o emergencia • Elaboración del Comité Asesor del Cambio (CAB) para	
--	-----------------------------------	---	---	--	---	--

	simule el ambiente de producción • Plan de marcha atrás (Back-out) para la recuperación ante un fallo • Implementar las nuevas versiones de software y hardware en el entorno de producción después de que la validación y pruebas las haya verificado			validar los cambios a implementar • Verificar el cumplimiento de las calendarizaciones propuestas • Verificar que la asignación de recursos es la adecuada • Definir al gestor de	
--	--	--	--	--	--

	en un entorno realista • Garantizar que el proceso de cambio cumpla con las especificaciones de la RFC • Asegurar que todos los cambios se ven correctamente reflejados • Implementar un control de versionamiento			cambios que sea el responsable del cambio • Evaluar las RFC para su aprobación • Planificar la gestión de cambios • Convocar a reunión del CAB para cambios menores y aprobación	
--	---	--	--	---	--

	• Pruebas del correcto funcionamiento de la versión • Pruebas de los manuales de instalación • Prueba de los planes de Back-out • Pruebas funcionales por los usuarios			n de las RFC • Establecer una política de implementación de nuevas versiones de hardware y software • Elaboración de un SLA • Elaboración de contratos de soporte		
--	---	--	--	--	--	--

						de servicios • Elaborar Plan de gestión de la demanda • Elaborar manual de evaluación del tipo de proveedor necesario para el servicio • Especificación de servicios que se ofrecerán		
--	--	--	--	--	--	--	--	--

					Verificación de la gestión del portafolio de servicios	
COBIT	- Se debe establecer un plan de adquisiciones de tecnología que se alinee con el plan de infraestructura tecnológica. - Se deben contar con procesos para	- Suministrar recursos TI de software. - Establecer procesos para la definición de requerimientos, planeación, desarrollo, pruebas y puesta en marcha de un nuevo software. - Establecer un proceso el cual permita la adquisición de	- Establecer políticas de acuerdo con el nivel de seguridad requerido. - Realizar copias de seguridad de datos regulares diariamente. Esa copia de seguridad podrá ser almacenada	- Establecer un plan de adquisición de servicios de comunicaciones acorde a las necesidades - Establecerse una	Llevar revisiones periódicas de las habilidades y competencias del recurso humano interno y externo.	- Se deben establecer procesos para desarrollar y transmitir la documentación de cada uno de los procesos de la organización. - Proporcionar acceso a repositorios

	actualizar la infraestructura tecnológica. • Se debe contar con un manual el cual establezca el uso del hardware por los usuarios. • Determinar la dirección tecnológica, mediante la creación de un plan de infraestructura tecnológica el cual	un software previo a un estudio donde se establezcan los requerimientos, y en base a las políticas de proveedores de la empresa. • Establecer un proceso el cual permita evaluar el desempeño actual del software en la organización y en base al grado de cumplimiento que estos den al negocio, se deberá establecer un	en un medio físico (por ejemplo, cinta o disco duro externo), o podría ser a una ubicación remota a través de la nube (es decir, Internet). • Controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas estén	política de adquisición de servicios de comunicación donde se estipulen las condiciones que el proveedor deberá cumplir. • Definir un plan estratégico o de TIC, el cual logre un balance	• Crear y mantener un inventario de recursos humanos de negocio y TI. • Utilizar la información financiera y de cartera para proporcionar datos de entrada a casos	de conocimiento para apoyar el desarrollo de habilidades y competencias.
--	--	--	--	--	---	---

	considere el número de equipos de TI con los que cuenta la empresa. • Evaluar el desempeño del hardware actual, a fin de establecer un plan de renovación de equipos. • Priorizar los recursos de TI para satisfacer los requerimientos en un	proceso para la actualización del software a una versión más reciente o su cambio por otra solución. • Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con las aplicaciones dentro del ambiente de producción, deben administrarse formal y	restringidos a usuarios autorizados. • Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información en toda la empresa. • Crear y mantener un inventario de información que incluya un listado de los	óptimo entre cubrir las necesidades del negocio y oportunidades tecnológicas. • Se deben establecer procesos para la evaluación, asignación de prioridad y autorizaciones de cambio.	de negocio para nuevas inversiones en activos y servicio de TI. • Establecer un órgano de toma de decisiones para priorizar recursos de TI y del negocio.
--	---	---	---	---	--

primer momento, así como para su crecimiento a corto y largo plazo. • Establecer políticas para revisar y autorizar las adquisiciones importantes de hardware, dentro de los límites aprobados por la junta directiva.	controladamente • Se deben establecer una metodología de pruebas sobre los nuevos desarrollos. • Mantener un registro de todas las licencias de software adquiridos y acuerdos de licencias asociados. • Llevar a cabo auditorías para identificar a todas las copias de software instalado con licencia.	propietarios, custodios y clasificación es. • Revisar acuerdos y políticas de los contratos. • Establecer un sistema de gestión de la calidad. • Definir y gestionar estándares, procesos y prácticas de calidad. • Supervisar y hacer controles y revisiones de la calidad.	• Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la gestión y ejecución de servicios de TI. • Analizar las actividades de los	
---	--	--	--	--

		• Gestión de errores y excepciones.	• Realizar un análisis de los riesgos potenciales y su impacto en el negocio. • Realizar escenarios de riesgos de TI. • Definir un portafolio de acciones a seguir para la gestión de riesgos. • Establecer y mantener un SGSI. • Definir y gestionar un plan de	procesos de negocio para identificar la necesidad de servicios de TI nuevos o rediseñados. • Definir y mantener los requerimientos técnicos y funcional es del negocio.	
--	--	---	--	--	--

				- Realizar estudios de viabilidad para proponer soluciones alternativas. - Identificar y registrar los activos actuales de TI. - Gestionar el ciclo de vida de los activos de TI.		
	tratamiento de riesgo de la seguridad de la información.	- Establecer y mantener una política de seguridad para las conexiones. - Cifrar la información en tránsito de acuerdo a su clasificación. - Aplicar protocolos de seguridad aprobados a las conexiones de red.				

				• Configurar sistemas operativos de forma segura. • Configurar los equipamientos de red en forma segura. • Realizar pruebas periódicas de la seguridad del sistema. • Implementar mecanismos de bloqueo a dispositivos. • Cifrar información de acuerdo	• Definir un esquema de clasificación para identificar todos los elementos de coste relacionados con TI. • Crear un presupuesto formal de TI, el cual incluya todos los costos relacionados a este		
--	--	--	--	---	---	--	--

			con su clasificación. • Gestionar el acceso y control remoto. • Proveer protección física a los dispositivos de usuario final. • Deshacerse de los dispositivos de usuario final de forma segura. • Asignar derechos de acceso y privilegios	rubro y el cual vaya alineado con la situación actual del negocio.		
--	--	--	--	---	--	--

				solo sobre lo que es necesario para ejecutar las actividades de trabajo, basado en roles de puestos predefinidos. • Revisar periódicamente la definición de los controles de acceso. • Identificar todos los procesos de negocio internos o sub			
--	--	--	--	---	--	--	--

				contratados que son críticos para las operaciones de la empresa o necesarios para cumplir las obligaciones legales y/o contractuales . • Identificar los procesos de soporte al negocio esenciales y servicios de TI. • Identificar escenarios				
--	--	--	--	--	--	--	--	--

				potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes Definir las acciones y comunicaciones en respuesta a incidentes que deben ser realizados en un evento de disrupción.			
ISO 27000	Se debe ubicar y	Se deben implementar	Se debe adoptar una	Periódica mente, la	Los anteced	Todos los empleados	

	proteger el equipo a fin de reducir los riesgos de amenazas y peligros ambientales y de oportunidad es de acceso no autorizado. Los equipos se protegerán contra los cortes de corriente y otras interrupcion es causadas por el fallo de las	procedimientos para controlar la instalación de software en los sistemas - Las modificaciones en los sistemas dentro del ciclo de vida del desarrollo deben controlarse mediante el uso de procedimientos formales de control de cambios. - Al cambiar las plataformas operativas, se deben revisar y	política y medidas de apoyo a la seguridad para manejar los riesgos introducidos por el uso de dispositivos móviles. Es preciso establecer una política y medidas de control de la seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles.	organización debe monitorear, revisar y revisar el servicio de entrega del proveedor . Hay que gestionar los cambios en la prestación de servicios por parte de los proveedor es, incluyend	entes de todos los candidatos al empleo deberán ser verificados de conformidad con las leyes, reglamentos y normas éticas pertinentes, y deberán ser proporci	de la empresa y, en su caso, los contratistas, deberían recibir una formación adecuada y una actualización periódica de las políticas y procedimientos de la empresa en relación con su función.
--	--	---	---	--	--	---

	herramientas de apoyo. - El cableado de energía y telecomunicaciones que transmite datos o soporta servicios de información debe estar protegido contra interceptación, interferencia u otros daños. - El estado del equipo debe ser objeto de un	probar las aplicaciones críticas para el negocio para asegurarse de que no haya un impacto adverso en las operaciones o la seguridad de la organización. Se debe desaconsejar la modificación de los conjuntos de programas informáticos, limitándolos a los cambios necesarios, y todos ellos deben estar	- Para habilitar los derechos de acceso, debe realizarse un proceso de registro y cancelación de usuarios. - Debe aplicarse un procedimiento estructurado de concesión de acceso a los usuarios con el fin de asignar o anular los derechos de acceso a todos los	o el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, tomando en cuenta la importancia crítica de la información, los	onales a los requisitos de la empresa, la clasificación de la información que se debe acceder y los riesgos percibidos. En los acuerdos contractuales
--	---	---	--	---	--

	mantenimiento adecuado para garantizar su continuidad, disponibilidad y integridad. - El equipo, la información o el software no se pueden retirar de las instalaciones sin una autorización previa. - Cuando se trabaje con equipos y recursos	estrictamente controlados. - En cualquier iniciativa de implementación de sistemas de información hay que establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros. - Las empresas deberán establecer y proteger de modo adecuado entornos de desarrollo seguros para las	tipos de usuarios a todos los sistemas y servicios. - La atribución y utilización de permisos de acceso privilegiado debe ser restringida y regulada. - Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un	sistemas y los procesos de la empresa implicados, así como la reevaluación de los riesgos. Se debe acordar con los proveedores y documentar los requisitos de seguridad de la información	con los empleados y contratos deben establecerse sus responsabilidades y las de la organización en materia de seguridad de la información. La gerencia debe
--	---	---	--	--	--

fuera de las instalaciones de la organización, las medidas de seguridad deben ser aplicadas teniendo en cuenta los riesgos involucrados. • Todos los equipos que dispongan de medios de almacenamiento deben ser verificados	iniciativas de desarrollo y la integración de sistemas durante todo el ciclo de vida del desarrollo. • El personal de la empresa tiene que supervisar y monitorear las actividades de desarrollo de sistemas subcontratados. • Durante el desarrollo del sistema es necesario realizar pruebas de la funcionalidad de seguridad.	proceso de gestión formal. • Los dueños de los recursos han de verificar periódicamente los derechos de acceso de los usuarios. • Se debe retirar a todos los empleados y a terceros el permiso de acceso a la información y a las instalaciones de	ón, para mitigar los riesgos asociados con el acceso de los proveedores a los recursos de la empresa. • Todos los requerimientos de seguridad de la información deben ser acordados con cada	requerir que los empleados y contratistas apliquen la seguridad de la información de conformidad con las políticas y procedimientos establecidos por la
---	--	---	---	--

	para garantizar que los datos confidenciales y el software con licencia han sido borrados o sobrescritos de manera segura antes de su reutilización o eliminación. • Debe garantizarse que el equipo desatendido tenga la	• Los programas de pruebas de aceptación y los criterios respectivos deben definirse para los nuevos sistemas de información, las actualizaciones y las nuevas versiones.	tratamiento de la información al término de la relación laboral, contrato o acuerdo, o bien adaptarlo después de un cambio. • Conviene restringir el acceso a la información y a las funcionalidades de los sistemas de aplicación de acuerdo con la política de	proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización. • Entre los acuerdos con los proveedores	organización. • Debe haber un proceso disciplinario formal y comunicado para las medidas que se tomen contra los empleados que hayan cometido una violación de la
--	--	---	---	---	--

	protección adecuada. • Es preciso establecer una política de escritorio limpio para los documentos y los soportes de almacenamiento extraíbles y otra para las instalaciones de procesamiento de la información.		control de acceso. • Cuando la política de control de acceso lo requiera, se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento de inicio de sesión seguro. • La gestión de contraseñas debe ser interactiva y garantizar la calidad de	es deben figurar requisitos para abordar los riesgos de seguridad de la información relacionados con los servicios de tecnología de la información y las comunicaciones.	seguridad de la información.
--	---	--	---	---	-------------------------------------

				las contraseñas. • Se debe restringir y controlar estrictamente el uso de programas de utilidad que podrían sobrescribir los controles de aplicaciones y sistemas. • El acceso al código fuente de los programas debe estar restringido. • Los controles de			
--	--	--	--	--	--	--	--

			detección, prevención y recuperación se deben implementar para proteger contra el software malicioso, combinado con una adecuada concienciación de los usuarios. • Se debe hacer una copia de seguridad de la información, el software y las imágenes		
--	--	--	--	--	--

				del sistema y comprobarla s periódicamente de acuerdo con la política de copias de seguridad. • Se debe seleccionar, proteger y supervisar cuidadosamente los datos de las pruebas.				
--	--	--	--	--	--	--	--	--

A.2.11 Instrumento 11

Unidad de análisis:	Buenas prácticas			
Variable:	Aplicabilidad			
Técnica:	Análisis de contenido			
Instrumento:	Lista de chequeo de buenas prácticas			
Objetivo:	Identificar aquellas buenas prácticas que son aplicables a la micro y pequeña empresa, basados en su clasificación.			
Lista de chequeo de buenas prácticas				
No.	Buena práctica	Microempresa Aplica (A) / No aplica (NA)	Pequeña empresa Aplica (A) / No aplica (NA)	Anotaciones
1	Gestión de incidencias y sus clasificaciones de urgencia e impacto de los servicios.	NA	NA	
2	Respaldo y restauración de archivos	A	A	
3	Gestión de impresión y salidas para la recopilación de documentos impresos u otros entregables electrónicos	NA	NA	
4	Actividades de rendimiento o mantenimiento en beneficio de los equipos	NA	NA	

5	Gestión de las instalaciones	NA	A	
6	Analizar el rendimiento de la infraestructura	NA	A	
7	Gestionar la demanda del servicio racionalizando su uso	NA	NA	
8	Proposición de mejoras en la infraestructura para aumentar la disponibilidad	NA	A	
9	Mantenimiento del servicio en operación y recuperación de este en caso de fallo	A	A	
10	Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios	NA	A	
11	Elaboración de RFC para iniciar actualización	NA	A	
12	Elaboración del plan de actualización	NA	NA	
13	Revisar la documentación del cambio a aplicar	A	A	
14	Comprobar los elementos de configuración	NA	NA	
15	Identificar todos los cambios que incluye la actualización	A	A	
16	Definir las fases y plazos de la ejecución del cambio	A	A	

17	Asignar los recursos para el cambio	A	A	A	
18	Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas	A		A	
19	Desarrollo de un ambiente de pruebas que simule el ambiente de producción	NA		NA	
20	Plan de marcha atrás (Back-out) para la recuperación ante un fallo	NA		NA	
21	Implementar las nuevas versiones de software y hardware en el entorno de producción después de que la validación y pruebas las haya verificado en un entorno realista	NA		NA	
22	Garantizar que el proceso de cambio cumpla con las especificaciones de la RFC	NA		A	
23	Asegurar que todos los cambios se ven correctamente reflejados	A		A	
24	Implementar un control de versionamiento	NA		A	
25	Pruebas del correcto funcionamiento de la versión	A		A	
26	Pruebas de los manuales de instalación	NA		A	

27	Prueba de los planes de Back-out	NA	NA	
28	Pruebas funcionales por los usuarios	A	A	
29	Elaborar política de seguridad	A	A	
30	Evaluación de riesgos contra la continuidad del servicio	NA	NA	
31	Elaborar Plan de seguridad	A	A	
32	Adoptar medidas proactivas de prevención de riesgos	A	A	
33	Desarrollar plan de contingencia	A	A	
34	Elaborar el plan de gestión de emergencias	NA	NA	
35	Elaborar el plan de recuperación	A	A	
37	Plan de inversión	NA	NA	
38	Debe evaluar costos reales asociados a la prestación de servicios	A	A	
39	Llevar la contabilidad de los gastos asociados	A	A	

40	Política de control de precios	NA	NA	NA	
41	Ofertas de servicios de otros proveedores	A		A	
42	Previsión de costes directos e indirectos de la creación y mantenimiento de cada servicio	NA		NA	
43	Realizar modelos de simulación de capacidad	NA		NA	
44	Elaboración de métricas de monitorización	A		A	
45	Diseño de evaluación de la arquitectura del servicio	NA		NA	
46	Desarrollar un plan de disponibilidad	A		A	
47	Diseño de paquetes de servicio	NA		NA	
48	Asesorar al cliente sobre el valor añadido que proporcionan los servicios de TI prestados	NA		NA	
49	Definir si es un servicio esencial	A		A	
50	Requisitos internos y externos a tener en cuenta	NA		NA	

51	Establecer la estrategia de continuidad	NA	NA	
52	Establecer política de continuidad	NA	NA	
53	Evaluar la capacidad de los proveedores internos y externos	A	A	
54	Definir si es un servicio de soporte	A	A	
55	Clasifica el tipo de entrega si es mayor, menor o emergencia	A	A	
56	Elaboración del Comité Asesor del Cambio (CAB) para validar los cambios a implementar	NA	NA	
57	Verificar el cumplimiento de las calendarizaciones propuestas	NA	NA	
58	Verificar que la asignación de recursos es la adecuada	A	A	
59	Definir al gestor de cambios que sea el responsable del cambio	NA	NA	
60	Evaluar las RFC para su aprobación	A	A	
61	Planificar la gestión de cambios	NA	NA	

62	Convocar a reunión del CAB para cambios menores y aprobación de las RFC	NA	NA	
63	Establecer una política de implementación de nuevas versiones de hardware y software	NA	NA	
64	Elaboración de un SLA	A	A	
65	Elaboración de contratos de soporte	A	A	
66	Determinar los requisitos de disponibilidad	A	A	
67	Elaboración del plan de capacidad	NA	NA	
68	Elaborar manual de requisitos de disponibilidad del negocio	NA	NA	
69	Elaboración del plan de entrega	NA	NA	
70	Crear documento para la petición de servicio (RFC, Request For Change)	A	A	
71	Elaborar Portafolio de servicios	NA	NA	
72	Elaborar Plan de gestión de la demanda	NA	NA	

73	Elaborar manual de evaluación del tipo de proveedor necesario para el servicio	A	A		
74	Especificación de servicios que se ofrecerán	A	A		
75	Verificación de la gestión del portafolio de servicios	NA	NA		
76	Crear un documento de gestión de accesos.	A	A		
77	Monitorear los recursos mediante los SLA	A	A		
78	Monitorear la disponibilidad evaluando el tiempo esperado versus tiempo de interrupción	A	A		
79	Consola de monitorización de equipos y servicios	NA	NA		
80	Documentar los recursos requeridos	A	A		
81	Monitorizar la disponibilidad del servicio	A	A		
82	Evaluación de la demanda	NA	A		
83	Evaluación de la utilidad	NA	NA		

84	Evaluación de la garantía	NA	NA	
85	Evaluación de externalización del servicio	A	A	
86	Evaluación de Inversión necesaria	A	A	
87	Evaluación del valor del servicio	A	A	
88	Evaluar el impacto de las políticas de seguridad en la disponibilidad	NA	NA	
89	Evaluar el impacto por interrupciones del servicio	NA	NA	
90	Evaluar los riesgos a los que está expuesta la infraestructura	NA	A	
91	Revisión del SLA	NA	NA	
92	Revisión de contratos de soporte	A	A	
93	Revisión del plan de capacidad	NA	NA	
94	Analizar el impacto a la continuidad del servicio	NA	NA	

95	Se debe ubicar y proteger el equipo a fin de reducir los riesgos de amenazas y peligros ambientales y de oportunidades de acceso no autorizado.	A	A	
96	Los equipos se protegerán contra los cortes de corriente y otras interrupciones causadas por el fallo de las herramientas de apoyo.	A	A	
97	El cableado de energía y telecomunicaciones que transmite datos o soporta servicios de información debe estar protegido contra interceptación, interferencia u otros daños.	NA	NA	
98	El estado del equipo debe ser objeto de un mantenimiento adecuado para garantizar su continuidad, disponibilidad e integridad.	A	A	
99	El equipo, la información o el software no se pueden retirar de las instalaciones sin una autorización previa.	A	A	
100	Cuando se trabaje con equipos y recursos fuera de las instalaciones de la organización, las medidas de seguridad deben ser aplicadas teniendo en cuenta los riesgos involucrados.	NA	NA	

101	Todos los equipos que dispongan de medios de almacenamiento deben ser verificados para garantizar que los datos confidenciales y el software con licencia han sido borrados o sobrescritos de manera segura antes de su reutilización o eliminación.	NA	NA	
102	Debe garantizarse que el equipo desatendido tenga la protección adecuada.	NA	NA	
103	Es preciso establecer una política de escritorio limpio para los documentos y los soportes de almacenamiento extraíbles y otra para las instalaciones de procesamiento de la información.	NA	NA	
104	Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.	NA	NA	
105	Las modificaciones en los sistemas dentro del ciclo de vida del desarrollo deben controlarse mediante el uso de procedimientos formales de control de cambios.	NA	NA	

106	Al cambiar las plataformas operativas, se deben revisar y probar las aplicaciones críticas para el negocio para asegurarse de que no haya un impacto adverso en las operaciones o la seguridad de la organización.	NA	NA	
107	Se debe desaconsejar la modificación de los conjuntos de programas informáticos, limitándolos a los cambios necesarios, y todos ellos deben estar estrictamente controlados.	A		
108	En cualquier iniciativa de implementación de sistemas de información hay que establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros.	NA	NA	
109	Las empresas deberán establecer y proteger de modo adecuado entornos de desarrollo seguros para las iniciativas de desarrollo y la integración de sistemas durante todo el ciclo de vida del desarrollo.	NA	NA	
110	El personal de la empresa tiene que supervisar y monitorizar las actividades de desarrollo de sistemas subcontratados.	A		
111	Durante el desarrollo del sistema es necesario realizar pruebas de la funcionalidad de seguridad.	NA	NA	

112	Los programas de pruebas de aceptación y los criterios respectivos deben definirse para los nuevos sistemas de información, las actualizaciones y las nuevas versiones.	NA	NA	
113	Se debe adoptar una política y medidas de apoyo a la seguridad para manejar los riesgos introducidos por el uso de dispositivos móviles.	A		
114	Es preciso establecer una política y medidas de control de la seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles.	NA		
115	Para habilitar los derechos de acceso, debe realizarse un proceso de registro y cancelación de usuarios.	A		
116	Debe aplicarse un procedimiento estructurado de concesión de acceso a los usuarios con el fin de asignar o anular los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.	NA		
117	La atribución y utilización de permisos de acceso privilegiado debe ser restringida y regulada.	A		

118	Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal.	NA	NA	
119	Los dueños de los recursos han de verificar periódicamente los derechos de acceso de los usuarios.	A		
120	Se debe retirar a todos los empleados y a terceros el permiso de acceso a la información y a las instalaciones de tratamiento de la información al término de la relación laboral, contrato o acuerdo, o bien adaptarlo después de un cambio.	A		
121	Conviene restringir el acceso a la información y a las funcionalidades de los sistemas de aplicación de acuerdo con la política de control de acceso.	NA	NA	
122	Cuando la política de control de acceso lo requiera, se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento de inicio de sesión seguro.	A	A	
123	La gestión de contraseñas debe ser interactiva y garantizar la calidad de las contraseñas.	A	A	

124	Se debe restringir y controlar estrictamente el uso de programas de utilidad que podrían sobrescribir los controles de aplicaciones y sistemas.	A	A	
125	El acceso al código fuente de los programas debe estar restringido.	NA	NA	
126	Los controles de detección, prevención y recuperación se deben implementar para proteger contra el software malicioso, combinado con una adecuada concienciación de los usuarios.	A	A	
127	Se debe hacer una copia de seguridad de la información, el software y las imágenes del sistema y comprobarlas periódicamente de acuerdo con la política de copias de seguridad.	A	A	
128	Se debe seleccionar, proteger y supervisar cuidadosamente los datos de las pruebas.	NA	NA	
129	Periódicamente, la organización debe monitorear y revisar el servicio de entrega del proveedor.	A	A	

130	Hay que gestionar los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, tomando en cuenta la importancia crítica de la información, los sistemas y los procesos de la empresa implicados, así como la reevaluación de los riesgos.	A	A	
131	Se debe acordar con los proveedores y documentar los requisitos de seguridad de la información, para mitigar los riesgos asociados con el acceso de los proveedores a los recursos de la empresa.	NA	NA	
132	Todos los requerimientos de seguridad de la información deben ser acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.	A	A	
133	Entre los acuerdos con los proveedores deben figurar requisitos para abordar los riesgos de seguridad de la información relacionados con los servicios de tecnología de la información y las comunicaciones.	NA	NA	

134	Los antecedentes de todos los candidatos al empleo deberán ser verificados de conformidad con las leyes, reglamentos y normas éticas pertinentes, y deberán ser proporcionales a los requisitos de la empresa, la clasificación de la información a la que se debe acceder y los riesgos percibidos.	A	A	
135	En los acuerdos contractuales con los empleados y contratistas deben establecerse sus responsabilidades y las de la organización en materia de seguridad de la información.	NA	NA	
136	La gerencia debe requerir que los empleados y contratistas apliquen la seguridad de la información de conformidad con las políticas y procedimientos establecidos por la organización.	A	A	
137	Debe haber un proceso disciplinario formal y comunicado para las medidas que se tomen contra los empleados que hayan cometido una violación de la seguridad de la información.	A	A	
138	Todos los empleados de la empresa y, en su caso, los contratistas, deberían recibir una formación adecuada y una actualización periódica de las políticas y procedimientos de la empresa en relación con su función.	A	A	

139	Se debe establecer un plan de adquisiciones de tecnología que se alinee con el plan de infraestructura tecnológica.	NA	NA	
140	Se deben contar con procesos para actualizar la infraestructura tecnológica.	NA	NA	
141	Se debe contar con un manual el cual establezca el uso del hardware por los usuarios.	A	A	
142	Determinar la dirección tecnológica, mediante la creación de un plan de infraestructura tecnológica el cual considere el número de equipos de TI con los que cuente la empresa.	A	A	
143	Evaluar el desempeño del hardware actual, a fin de establecer un plan de renovación de equipos.	NA	NA	
144	Priorizar los recursos de TI para satisfacer los requerimientos en un primer momento, así como para su crecimiento a corto y largo plazo.	NA	NA	
145	Establecer políticas para revisar y autorizar las adquisiciones importantes de hardware, dentro de los límites aprobados por la junta directiva.	A	A	
146	Suministrar recursos TI de software.	A	A	

147	Establecer procesos para la definición de requerimientos, planeación, desarrollo, pruebas y puesta en marcha de un nuevo software.	A		A	
148	Establecer un proceso el cual permita la adquisición de un software previo a un estudio donde se establezcan los requerimientos, y en base a las políticas de proveedores de la empresa.	A		A	
149	Establecer un proceso el cual permita evaluar el desempeño actual del software en la organización y en base al grado de cumplimiento que estos den al negocio, se deberá establecer un proceso para la actualización del software a una versión más reciente o su cambio por otra solución.	A		A	
150	Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente.	NA		NA	
151	Se deben establecer una metodología de pruebas sobre los nuevos desarrollos.	A		A	
152	Mantener un registro de todas las licencias de software adquiridos y acuerdos de licencias asociados.	A		A	

153	Llevar a cabo auditorias para identificar a todas las copias de software instalado con licencia.	A	A	
154	Gestión de errores y excepciones.	A	A	
155	Establecer políticas de acuerdo con el nivel de seguridad requerido.	A	A	
156	Realizar copias de seguridad de datos regulares diariamente. Esa copia de seguridad podrá ser almacenada en un medio físico (por ejemplo, cinta o disco duro externo), o podría ser a una ubicación remota a través de la nube (es decir, Internet).	A	A	
157	Controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas estén restringidos a usuarios autorizados.	A	A	
158	Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información en toda la empresa.	NA	NA	
159	Crear y mantener un inventario de información que incluya un listado de los propietarios, custodios y clasificaciones.	NA	NA	
160	Revisar acuerdos y políticas de los contratos.	A	A	

161	Establecer un sistema de gestión de la calidad.	NA	NA		
162	Definir y gestionar estándares, procesos y prácticas de calidad.	NA	NA		
163	Supervisar y hacer controles y revisiones de la calidad.	NA	NA		
164	Realizar un análisis de los riesgos potenciales y su impacto en el negocio.	A	A		
165	Realizar escenarios de riesgos de TI.	NA	NA		
166	Definir un portafolio de acciones a seguir para la gestión de riesgos.	NA	NA		
167	Establecer y mantener un SGSI.	NA	NA		
168	Definir y gestionar un plan de tratamiento de riesgo de la seguridad de la información.	NA	NA		
169	Establecer y mantener una política de seguridad para las conexiones.	A	A		
170	Cifrar la información en tránsito de acuerdo a su clasificación.	NA	NA		
171	Aplicar protocolos de seguridad aprobados a las conexiones de red.	NA	NA		
172	Configurar sistemas operativos de forma segura.	A	A		

173	Configurar los equipamientos de red en forma segura.	A	A		
174	Realizar pruebas periódicas de la seguridad del sistema.	A	A		
175	Implementar mecanismos de bloqueo a dispositivos.	A	A		
176	Cifrar información de acuerdo con su clasificación.	NA	NA		
177	Gestionar el acceso y control remoto.	A	A		
178	Proveer protección física a los dispositivos de usuario final.	A	A		
179	Desahacerse de los dispositivos de usuario final de forma segura.	A	A		
180	Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basado en roles de puestos predefinidos.	A	A		
181	Revisar periódicamente la definición de los controles de acceso.	A	A		
182	Identificar todos los procesos de negocio internos o sub contratados que son críticos para las operaciones de la empresa o necesarios para cumplir las obligaciones legales y/o contractuales.	A	A		

183	Identificar los procesos de soporte al negocio esenciales y servicios de TI.	A	A		
184	Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes	A	A		
185	Definir las acciones y comunicaciones en respuesta a incidentes que deben ser realizados en un evento de disrupción.	A	A		
186	Establecer un plan de adquisición de servicios de comunicaciones acorde a las necesidades actuales.	A	A		
187	Establecerse una política de adquisición de servicios de comunicación en donde se estipulen las condiciones que el proveedor deberá cumplir.	A	A		
188	Definir un plan estratégico de TIC, el cual logre un balance óptimo entre cubrir las necesidades del negocio y oportunidades tecnológicas.	A	A		
189	Se deben establecer procesos para la evaluación, asignación de prioridad y autorizaciones de cambio.	A	A		
190	Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la gestión y ejecución de servicios de TI.	NA	NA		

191	Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios de TI nuevos o rediseñados.	A	A	
192	Definir y mantener los requerimientos técnicos y funcionales del negocio.	A	A	
193	Realizar estudios de viabilidad para proponer soluciones alternativas.	NA	NA	
194	Identificar y registrar los activos actuales de TI.	A	A	
195	Gestionar el ciclo de vida de los activos de TI.	A	A	
196	Definir un esquema de clasificación para identificar todos los elementos de coste relacionados con TI.	A	A	
197	Crear un presupuesto formal de TI, el cual incluya todos los costos relacionados a este rubro y el cual vaya alineado con la situación actual del negocio.	A	A	
198	Llevar revisiones periódicas de las habilidades y competencias del recurso humano interno y externo.	A	A	
199	Crear y mantener un inventario de recursos humanos de negocio y TI.	A	A	

200	Utilizar la información financiera y de cartera para proporcionar datos de entrada a casos de negocio para nuevas inversiones en activos y servicios de TI.	NA	NA		
201	Establecer un órgano de toma de decisiones para priorizar recursos de TI y del negocio.	NA	NA		
202	Se deben establecer procesos para desarrollar y transmitir la documentación de cada uno de los procesos de la organización.	A	A		
203	Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias.	NA	NA		

A.2.12 Instrumento 12

Unidad de análisis:	Modelo de aplicación	
Variable:	Presupuesto	
Técnica:	Análisis de contenido	
Instrumento:	Matriz de costos	
Objetivo:	Realizar una estimación del costo de la implementación completa de este modelo.	
Matriz de costos		
Buena práctica		Costo de implementación mínimo anual (\$)
Mantenimiento del servicio en operación y recuperación de este en caso de fallo		\$ 3,000.00
Revisar la documentación del cambio a aplicar		\$ -
Identificar todos los cambios que incluye la actualización *		\$ -
Definir las fases y plazos de la ejecución del cambio **		\$ -
Asignar los recursos para el cambio **		\$ -
Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas *		\$ -
Asegurar que todos los cambios se ven correctamente reflejados *		\$ -
Pruebas del correcto funcionamiento de la versión *		\$ -
Pruebas funcionales por los usuarios		\$ -
Elaborar política de seguridad		\$ 100.00
Elaborar Plan de seguridad *		\$ -
Adoptar medidas proactivas de prevención de riesgos		\$ 200.00
Desarrollar plan de contingencia *		\$ -
Elaborar el plan de recuperación *		\$ -

Debe evaluar costos reales asociados a la prestación de servicios **	\$	-
Llevar la contabilidad de los gastos asociados **	\$	-
Ofertas de servicios de otros proveedores **	\$	-
Elaboración de métricas de monitorización *	\$	-
Desarrollar un plan de disponibilidad *	\$	-
Definir si es un servicio esencial *	\$	-
Evaluar la capacidad de los proveedores internos y externos **	\$	-
Definir si es un servicio de soporte *	\$	-
Clasifica el tipo de entrega si es mayor, menor o emergencia *	\$	-
Verificar que la asignación de recursos es la adecuada *	\$	-
Crear documento para la petición de servicio (RFC, Request For Change) **	\$	-
Evaluar las RFC para su aprobación **	\$	-
Elaboración de un SLA *	\$	-
Elaboración de contratos de soporte *	\$	-
Determinar los requisitos de disponibilidad *	\$	-
Elaborar manual de evaluación del tipo de proveedor necesario para el servicio **	\$	-
Especificación de servicios que se ofrecerán *	\$	-
Crear un documento de gestión de accesos *	\$	-
Monitorizar los recursos mediante los SLA *	\$	-
Monitorizar la disponibilidad evaluando el tiempo esperado versus tiempo de interrupción *	\$	-
Documentar los recursos requeridos *	\$	-
Monitorizar la disponibilidad del servicio *	\$	-
Evaluación de externalización del servicio *	\$	-
Evaluación de Inversión necesaria **	\$	-
Evaluación del valor del servicio *	\$	-
Revisión de contratos de soporte **	\$	-
Se debe ubicar y proteger el equipo a fin de reducir los riesgos de amenazas y peligros ambientales y de oportunidades de acceso no autorizado *	\$	-

Los equipos se protegerán contra los cortes de corriente y otras interrupciones causadas por el fallo de las herramientas de apoyo.	\$	30.00
El estado del equipo debe ser objeto de un mantenimiento adecuado para garantizar su continuidad, disponibilidad e integridad. *	\$	-
El equipo, la información o el software no se pueden retirar de las instalaciones sin una autorización previa	\$	-
Se debe desaconsejar la modificación de los conjuntos de programas informáticos, limitándolos a los cambios necesarios, y todos ellos deben estar estrictamente controlados.	\$	-
El personal de la empresa tiene que supervisar y monitorear las actividades de desarrollo de sistemas subcontratados. **	\$	-
Se debe adoptar una política y medidas de apoyo a la seguridad para manejar los riesgos introducidos por el uso de dispositivos móviles. **	\$	-
Para habilitar los derechos de acceso, debe realizarse un proceso de registro y cancelación de usuarios. **	\$	-
La atribución y utilización de permisos de acceso privilegiado debe ser restringida y regulada. **	\$	-
Los dueños de los recursos han de verificar periódicamente los derechos de acceso de los usuarios.	\$	-
Se debe retirar a todos los empleados y a terceros el permiso de acceso a la información y a las instalaciones de tratamiento de la información al término de la relación laboral, contrato o acuerdo, o bien adaptarlo después de un cambio. **	\$	-
Cuando la política de control de acceso lo requiera, se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento de inicio de sesión seguro.	\$	-
La gestión de contraseñas debe ser interactiva y garantizar la calidad de las contraseñas.	\$	-
Se debe restringir y controlar estrictamente el uso de programas de utilidad que podrían sobrescribir los controles de aplicaciones y sistemas.	\$	-
Los controles de detección, prevención y recuperación se deben implementar para proteger contra el software malicioso, combinado con una adecuada concienciación de los usuarios.	\$	7.50
Se debe hacer una copia de seguridad de la información, el software y las imágenes del sistema y comprobarlas periódicamente de acuerdo con la política de copias de seguridad. *	\$	-
Periódicamente, la organización debe monitorear y revisar el servicio de entrega del proveedor. **	\$	-

Hay que gestionar los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, tomando en cuenta la importancia crítica de la información, los sistemas y los procesos de la empresa implicados, así como la reevaluación de los riesgos. **	\$	-
Todos los requerimientos de seguridad de la información deben ser acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización. **	\$	-
Los antecedentes de todos los candidatos al empleo deberán ser verificados de conformidad con las leyes, reglamentos y normas éticas pertinentes, y deberán ser proporcionales a los requisitos de la empresa, la clasificación de la información a la que se debe acceder y los riesgos percibidos. **	\$	-
La gerencia debe requerir que los empleados y contratistas apliquen la seguridad de la información de conformidad con las políticas y procedimientos establecidos por la organización. **	\$	-
Debe haber un proceso disciplinario formal y comunicado para las medidas que se tomen contra los empleados que hayan cometido una violación de la seguridad de la información. **	\$	-
Todos los empleados de la empresa y, en su caso, los contratistas, deberían recibir una formación adecuada y una actualización periódica de las políticas y procedimientos de la empresa en relación con su función. **	\$	-
Se debe contar con un manual el cual establezca el uso del hardware por los usuarios.	\$	-
Determinar la dirección tecnológica, mediante la creación de un plan de infraestructura tecnológica el cual considere el número de equipos de TI con los que cuente la empresa. **	\$	-
Establecer políticas para revisar y autorizar las adquisiciones importantes de hardware, dentro de los límites aprobados por la junta directiva. **	\$	-
Suministrar recursos TI de software. **	\$	-
Establecer procesos para la definición de requerimientos, planeación, desarrollo, pruebas y puesta en marcha de un nuevo software. *	\$	-
Establecer un proceso el cual permita la adquisición de un software previo a un estudio donde se establezcan los requerimientos, y en base a las políticas de proveedores de la empresa. **	\$	-

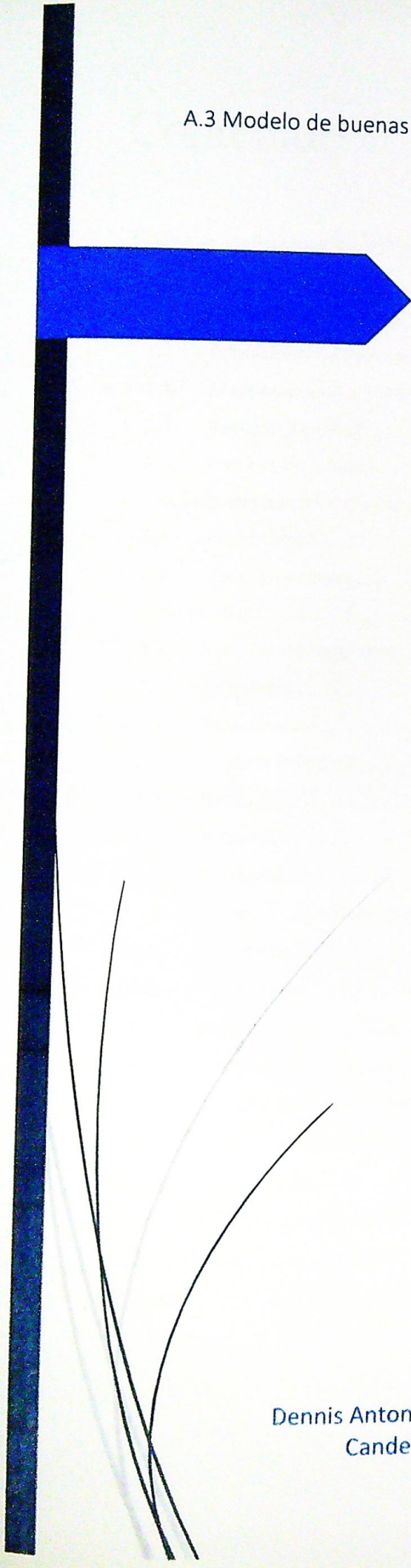
Establecer un proceso el cual permita evaluar el desempeño actual del software en la organización y en base al grado de cumplimiento que estos den al negocio, se deberá establecer un proceso para la actualización del software a una versión más reciente o su cambio por otra solución. **	\$	-
Se deben establecer una metodología de pruebas sobre los nuevos desarrollos. **	\$	-
Mantener un registro de todas las licencias de software adquiridos y acuerdos de licencias asociados. **	\$	-
Llevar a cabo auditorías para identificar a todas las copias de software instalado con licencia. **	\$	-
Gestión de errores y excepciones. **	\$	-
Establecer políticas de acuerdo con el nivel de seguridad requerido. **	\$	-
Realizar copias de seguridad de datos regulares diariamente. Esa copia de seguridad podrá ser almacenada en un medio físico (por ejemplo, cinta o disco duro externo), o podría ser a una ubicación remota a través de la nube (es decir, Internet).	\$	72.00
Controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas estén restringidos a usuarios autorizados. **	\$	-
Revisar acuerdos y políticas de los contratos. **	\$	-
Realizar un análisis de los riesgos potenciales y su impacto en el negocio. **	\$	-
Establecer y mantener una política de seguridad para las conexiones. **	\$	-
Configurar sistemas operativos de forma segura. *	\$	-
Configurar los equipamientos de red en forma segura. *	\$	-
Realizar pruebas periódicas de la seguridad del sistema. *	\$	-
Implementar mecanismos de bloqueo a dispositivos. *	\$	-
Gestionar el acceso y control remoto. **	\$	-
Proveer protección física a los dispositivos de usuario final. *	\$	-
Deshacerse de los dispositivos de usuario final de forma segura. *	\$	-
Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basado en roles de puestos predefinidos. **	\$	-
Revisar periódicamente la definición de los controles de acceso. **	\$	-
Identificar todos los procesos de negocio internos o sub contratados que son críticos para las operaciones de la empresa o necesarios para cumplir las obligaciones legales y/o contractuales. **	\$	-

Identificar los procesos de soporte al negocio esenciales y servicios de TI. **	\$	-
Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes. **	\$	-
Definir las acciones y comunicaciones en respuesta a incidentes que deben ser realizados en un evento de disrupción. **	\$	-
Establecer un plan de adquisición de servicios de comunicaciones acorde a las necesidades actuales. **	\$	-
Establecerse una política de adquisición de servicios de comunicación en donde se estipulen las condiciones que el proveedor deberá cumplir. **	\$	-
Definir un plan estratégico de TIC, el cual logre un balance optimo entre cubrir las necesidades del negocio y oportunidades tecnológicas. **	\$	-
Se deben establecer procesos para la evaluación, asignación de prioridad y autorizaciones de cambio. **	\$	-
Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios de TI nuevos o rediseñados. **	\$	-
Definir y mantener los requerimientos técnicos y funcionales del negocio. *	\$	-
Identificar y registrar los activos actuales de TI. **	\$	-
Gestionar el ciclo de vida de los activos de TI. **	\$	-
Definir un esquema de clasificación para identificar todos los elementos de coste relacionados con TI. **	\$	-
Crear un presupuesto formal de TI, el cual incluya todos los costos relacionados a este rubro y el cual vaya alineado con la situación actual del negocio. **	\$	-
Llevar revisiones periódicas de las habilidades y competencias del recurso humano interno y externo. **	\$	-
Crear y mantener un inventario de recursos humanos de negocio y TI. **	\$	-
Se deben establecer procesos para desarrollar y transmitir la documentación de cada uno de los procesos de la organización. **	\$	-
Total implementación anual:	\$3,481.50	

NOTA:

* Costo será absorbido por el especialista TIC.

** Actividades administrativas sin costo para la organización.



Manual de buenas prácticas para las tecnologías de la información y comunicaciones (TIC) para la micro y pequeña empresa en El Salvador

MYPETIC 1.0

Dennis Antonio Pérez Escobar; Emerson Francisco Cartagena
Candelario; Hector Alexander Valladares Pérez

Contenido

Proceso de implementación del manual	1
Buenas prácticas	2
1 Administración de Hardware	2
1.1 Adquisición de equipos	2
1.2 Mantenimiento y soporte técnico.....	2
1.3 Revisión y control	2
1.4 Pruebas de equipos	2
2 Administración de software	3
2.1 Planificación	3
2.2 Revisión y control	3
3 Seguridad.....	4
3.1 Políticas de Seguridad	4
3.2 Respaldos	4
3.3 Restauración.....	4
3.4 Soporte Helpdesk	4
3.5 Redes	5
3.6 Antivirus	5
3.7 Auditoria.....	5
4 Administración de los servicios relacionados a TIC.....	6
4.1 Financiero	6
4.2 Proveedores	6
4.3 Monitoreo	7
4.4 Planificación	7
4.5 Nuevos servicios y actualizaciones.....	7
4.6 Servicios en operación.....	7
5 Recursos humanos	8
6 Gestión del conocimiento	9
Consideraciones	9
Bibliografía.....	

Introducción

En la actualidad, la manera de hacer negocios se ve influenciada directamente por las tecnologías de información; constantemente se observa cómo se hacen negocios a través de aplicaciones móviles, redes sociales, páginas web, correos electrónicos y programas colaborativos que permiten conectar personas y mercados cada vez más diversos. Las tecnologías de información y comunicaciones (TIC) se han convertido en un aliado estratégico para las empresas, y, por tanto, un área que necesita de mucha atención y control debido a su constante actualización e innovación.

Las micro y pequeñas empresas, por su categorización no son ajenas a las TIC y cada una de ellas cuenta con al menos un servicio de tecnología (Internet, correo electrónico, aplicación móvil, red social, etc.), pero no existe un control sobre estos, y cuando no se tiene controlado se pueden incurrir en gastos innecesarios en servicios de tecnología de información (TI) o se pueden perder oportunidades de negocio por la falta de herramientas adecuadas (no necesariamente costosas).

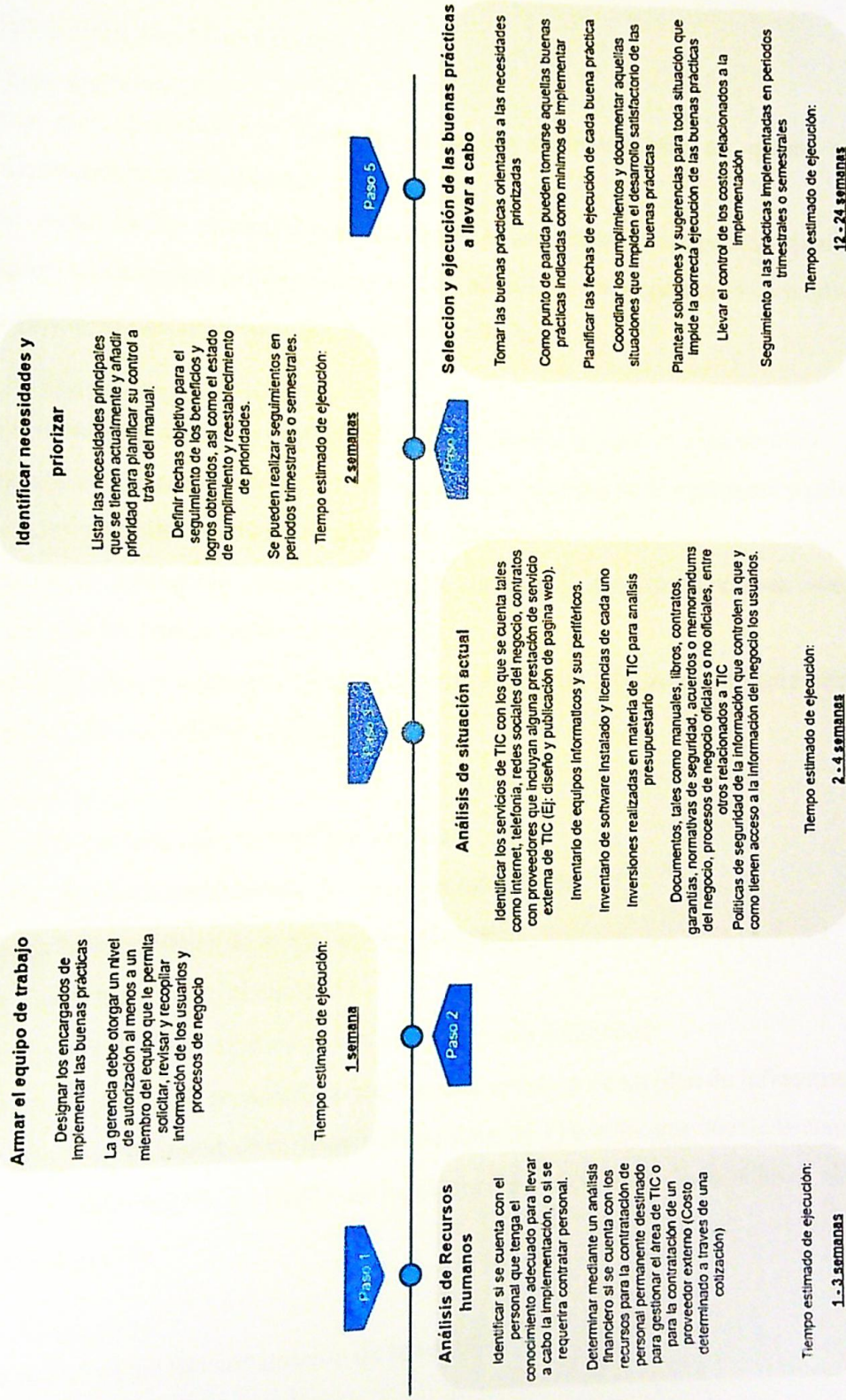
La gestión de las TIC en las micro y pequeñas empresas no es una actividad directamente planificada, y en muchas ocasiones, dado el concepto de costoso, no se cuenta con personal o contratos que apoyen esta tarea tan importante. Mantenimiento de equipos informáticos, verificación de conectividad de internet, administración de accesos a los archivos o programas en uso, control de licencias, administración de contratos con proveedores, etc., por mencionar algunas, son actividades que necesitan atención ya que forman parte de la estrategia de los negocios, y que, en alguna medida, aportan al crecimiento económico y aumento en la competitividad de las empresas.

Este manual cuenta con buenas prácticas tomadas de metodologías orientadas a la administración de servicios de TI, gobierno corporativo y seguridad de la información, todas ellas, en función de alinearse a las capacidades y necesidades fundamentales de las micro y pequeña empresa de El Salvador, esto, con el objetivo de apoyar a que este sector económico del país tenga claridad de su situación actual de TIC y una visión de hacia dónde deben encaminarse, sin forzar o poner en riesgo los procesos de negocio, al contrario, que estratégicamente cada práctica agregue valor para su crecimiento.

Adicionalmente se añade un proceso de implementación general que integra los elementos básicos y primordiales que se deben tomar en cuenta para iniciar y ejecutar la implementación

de este manual. Se describen 5 pasos de implementación donde cada uno contiene temáticas que deben ser abordadas, esto permitirá tener una idea introductoria que guía por donde comenzar y lo que cada paso debe ejecutar como mínimo.

Proceso de implementación del manual



Buenas prácticas

1 Administración de Hardware

1.1 Adquisición de equipos

- Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas
- Se debe contar con un manual el cual establezca el uso del hardware por los usuarios.
- Establecer políticas para revisar y autorizar las adquisiciones importantes de hardware, dentro de los límites aprobados por la junta directiva.

1.2 Mantenimiento y soporte técnico

- Mantenimiento del servicio en operación y recuperación de este en caso de fallo
- Se debe ubicar y proteger el equipo a fin de reducir los riesgos de amenazas y peligros ambientales y de oportunidades de acceso no autorizado.
- Los equipos se protegerán contra los cortes de corriente y otras interrupciones causadas por el fallo de las herramientas de apoyo. *
- El estado del equipo debe ser objeto de un mantenimiento adecuado para garantizar su continuidad, disponibilidad e integridad.

1.3 Revisión y control

- Revisar la documentación del cambio a aplicar
- Identificar todos los cambios que incluye la actualización
- Definir las fases y plazos de la ejecución del cambio
- Asignar los recursos para el cambio
- Asegurar que todos los cambios se ven correctamente reflejados
- Determinar la dirección tecnológica, mediante la creación de un plan de infraestructura tecnológica el cual considere el número de equipos de TI con los que cuenta la empresa.
- El equipo, la información o el software no se pueden retirar de las instalaciones sin una autorización previa.

1.4 Pruebas de equipos

- Pruebas del correcto funcionamiento de la versión
- Pruebas funcionales por los usuarios

2 Administración de software

2.1 Planificación

- Definir las fases y plazos de la ejecución del cambio
- Identificar todos los cambios que incluye la actualización
- Establecer procesos para la definición de requerimientos, planeación, desarrollo, pruebas y puesta en marcha de un nuevo software.
- Establecer un proceso el cual permita evaluar el desempeño actual del software en la organización y en base al grado de cumplimiento que estos den al negocio, se deberá establecer un proceso para la actualización del software a una versión más reciente o su cambio por otra solución.
- Se deben establecer una metodología de pruebas sobre los nuevos desarrollos.
- Establecer un proceso el cual permita la adquisición de un software previo a un estudio donde se establezcan los requerimientos, y en base a las políticas de proveedores de la empresa.
- Asignar los recursos para el cambio
- Suministrar recursos TI de software.

2.2 Revisión y control

- Revisar la documentación del cambio a aplicar
- Asegurar que el software y hardware adquirido o desarrollado se ajustan a las especificaciones predeterminadas
- Asegurar que todos los cambios se ven correctamente reflejados
- Pruebas funcionales por los usuarios
- Pruebas del correcto funcionamiento de la versión
- Llevar a cabo auditorias para identificar a todas las copias de software instalado con licencia.
- Mantener un registro de todas las licencias de software adquiridos y acuerdos de licencias asociados.
- El personal de la empresa tiene que supervisar y monitorear las actividades de desarrollo de sistemas subcontratados.
- Mantenimiento del servicio en operación y recuperación de este en caso de fallo
- Gestión de errores y excepciones.

- Se debe desaconsejar la modificación de los conjuntos de programas informáticos, limitándolos a los cambios necesarios, y todos ellos deben estar estrictamente controlados.

3 Seguridad

3.1 Políticas de Seguridad

- Elaborar política de seguridad
- Adoptar medidas proactivas de prevención de riesgos
- Desarrollar plan de contingencia
- Elaborar el plan de recuperación
- Establecer políticas de acuerdo con el nivel de seguridad requerido.
- Revisar acuerdos y políticas de los contratos.
- Establecer y mantener una política de seguridad para las conexiones.
- Identificar los procesos de soporte al negocio esenciales y servicios de TI. *
- Se debe adoptar una política y medidas de apoyo a la seguridad para manejar los riesgos introducidos por el uso de dispositivos móviles.

3.2 Respaldos

- Respaldo de archivos. *
- Realizar copias de seguridad de datos regulares diariamente. Esa copia de seguridad podrá ser almacenada en un medio físico (por ejemplo, cinta o disco duro externo), o podría ser a una ubicación remota a través de la nube (es decir, Internet).
- Se debe hacer una copia de seguridad de la información, el software y las imágenes del sistema y comprobarlas periódicamente de acuerdo con la política de copias de seguridad.
- Definir las acciones y comunicaciones en respuesta a incidentes que deben ser realizados en un evento de interrupción.

3.3 Restauración

- Plan de recuperación

3.4 Soporte Helpdesk

- Controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas estén restringidos a usuarios autorizados.
- Configurar sistemas operativos de forma segura.
- Realizar pruebas periódicas de la seguridad del sistema.

- Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basado en roles de puestos predefinidos.
- Revisar periódicamente la definición de los controles de acceso.
- Proveer protección física a los dispositivos de usuario final.
- Deshacerse de los dispositivos de usuario final de forma segura.
- La gestión de contraseñas debe ser interactiva y garantizar la calidad de las contraseñas.
- Se debe restringir y controlar estrictamente el uso de programas de utilidad que podrían sobrescribir los controles de aplicaciones y sistemas.
- Para habilitar los derechos de acceso, debe realizarse un proceso de registro y cancelación de usuarios.
- La atribución y utilización de permisos de acceso privilegiado debe ser restringida y regulada.
- Los dueños de los recursos han de verificar periódicamente los derechos de acceso de los usuarios.
- Se debe retirar a todos los empleados y a terceros el permiso de acceso a la información y a las instalaciones de tratamiento de la información al término de la relación laboral, contrato o acuerdo, o bien adaptarlo después de un cambio.
- Cuando la política de control de acceso lo requiera, se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento de inicio de sesión seguro.

3.5 Redes

- Implementar mecanismos de bloqueo a dispositivos.
- Configurar los equipamientos de red en forma segura.
- Gestionar el acceso y control remoto.

3.6 Antivirus

- Los controles de detección, prevención y recuperación se deben implementar para proteger contra el software malicioso, combinado con una adecuada concienciación de los usuarios.

3.7 Auditoria

- Realizar un análisis de los riesgos potenciales y su impacto en el negocio.
- Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes

- Identificar todos los procesos de negocio internos o sub contratados que son críticos para las operaciones de la empresa o necesarios para cumplir las obligaciones legales y/o contractuales.

4 Administración de los servicios relacionados a TIC

4.1 Financiero

- Debe evaluar costos reales asociados a la prestación de servicios. *
- Llevar la contabilidad de los gastos asociados
- Definir un esquema de clasificación para identificar todos los elementos de coste relacionados con TI.
- Crear un presupuesto formal de TI, el cual incluya todos los costos relacionados a este rubro y el cual vaya alineado con la situación actual del negocio.

4.2 Proveedores

- Ofertas de servicios de otros proveedores
- Evaluar la capacidad de los proveedores internos y externos
- Elaboración de un SLA
- Elaboración de contratos de soporte
- Elaborar manual de evaluación del tipo de proveedor necesario para el servicio
- Establecerse una política de adquisición de servicios de comunicación en donde se estipulen las condiciones que el proveedor deberá cumplir.
- Hay que gestionar los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, tomando en cuenta la importancia crítica de la información, los sistemas y los procesos de la empresa implicados, así como la reevaluación de los riesgos.
- Todos los requerimientos de seguridad de la información deben ser acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.

4.3 Monitoreo

- Elaboración de métricas de monitorización
- Periódicamente, la organización debe monitorear, revisar y revisar el servicio de entrega del proveedor.

4.4 Planificación

- Desarrollar un plan de disponibilidad
- Establecer un plan de adquisición de servicios de comunicaciones acorde a las necesidades actuales.
- Se deben establecer procesos para la evaluación, asignación de prioridad y autorizaciones de cambio.
- Definir un plan estratégico de TIC, el cual logre un balance optimo entre cubrir las necesidades del negocio y oportunidades tecnológicas.
- Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios de TI nuevos o rediseñados.
- Definir y mantener los requerimientos técnicos y funcionales del negocio.

4.5 Nuevos servicios y actualizaciones

- Crear documento para la petición de servicio (RFC, Request For Change)
- Evaluar las RFC para su aprobación
- Definir si es un servicio esencial
- Definir si es un servicio de soporte
- Verificar que la asignación de recursos es la adecuada
- Especificación de servicios que se ofrecerán
- Determinar los requisitos de disponibilidad
- Clasificar el tipo de entrega si es mayor, menor o emergencia

4.6 Servicios en operación

- Identificar y registrar los activos actuales de TI. *
- Gestionar el ciclo de vida de los activos de TI.

5 Recursos humanos

- Crear un documento de gestión de accesos. *
- Llevar revisiones periódicas de las habilidades y competencias del recurso humano interno y externo.
- Crear y mantener un inventario de recursos humanos de negocio y TI.
- Los antecedentes de todos los candidatos al empleo deberán ser verificados de conformidad con las leyes, reglamentos y normas éticas pertinentes, y deberán ser proporcionales a los requisitos de la empresa, la clasificación de la información a la que se debe acceder y los riesgos percibidos.

- La gerencia debe requerir que los empleados y contratistas apliquen la seguridad de la información de conformidad con las políticas y procedimientos establecidos por la organización.
- Debe haber un proceso disciplinario formal y comunicado para las medidas que se tomen contra los empleados que hayan cometido una violación de la seguridad de la información.

6 Gestión del conocimiento

- Monitorear los recursos mediante los SLA
- Monitorear la disponibilidad evaluando el tiempo esperado versus tiempo de interrupción
- Documentar los recursos requeridos
- Monitorizar la disponibilidad del servicio
- Evaluación de la demanda
- Evaluación de externalización del servicio
- Evaluación de Inversión necesaria
- Evaluación del valor del servicio
- Revisión de contratos de soporte
- Todos los empleados de la empresa y, en su caso, los contratistas, deberían recibir una formación adecuada y una actualización periódica de las políticas y procedimientos de la empresa en relación con su función.

NOTA:

* Las buenas prácticas que como mínimo debería de cumplir la organización.

Consideraciones

- Para garantizar la correcta implementación de las buenas prácticas, se sugiere realizar revisiones periódicas trimestrales durante el primer año, posteriormente, con las buenas prácticas encaminadas y adoptadas, podrían llevarse a cabo semestralmente. Es importante tener claro que estas revisiones no deben abandonarse por ningún motivo ya que son la principal fuente de información que indique cuando se es
- Tal como se indica en el proceso de implementación, cada paso detalla un tiempo en semanas, determinando un periodo de 1 a 3 años para una implementación total del manual; tomando en cuenta que el tiempo está relacionado a la diversidad y amplitud de los servicios TIC de la empresa, así como también de las necesidades identificadas en el análisis de situación actual.
- La persona encargada de la implementación de este manual ya sea recurso interno o subcontratado, deberá cumplir con el siguiente perfil:
 - Formación académica referente a la rama de la informática.
 - Conocimiento de los requisitos y aplicación de la norma ISO 27001 y las metodologías COBIT e ITIL.
 - Al menos 3 años de experiencia en el ámbito de las TIC.

Bibliografía

Amir, H., & Ronen, M. (2013). Conducting ethical yet realistic usable security studies.

Bailey, C. (2010). *ITIL Version 3, manual técnico de fundamentos*.

COBIT "Objetivos de Control para la Información y la Tecnología relacionada". (19 de Marzo de 2017). Obtenido de <http://cobitzd.blogspot.com/2017/03/dominios.html>

INCIBE. (15 de 02 de 2019). *Buenas prácticas en el área informática. Colección: Protege tu empresa*.