UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"PROPUESTA DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA DESYSWEB S.A.C. EN EL PERIODO 2017"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR BACHILLER
MASCCO TOMAIRO, DIANA ESTHER

Villa El Salvador
2017

DEDICATORIA

En primer lugar a nuestro creador, a mis padres Wilfredo y Lourdes, especialmente a mi abuela Juana y a mi hermano por su apoyo incondicional para poder llegar a ser un buen profesional.

AGRADECIMIENTO

Quiero agradecer en primer lugar a la Universidad Nacional Tecnológica De Lima Sur (UNTELS) por haberme aceptado y ser parte de ella así mismo al abrirme las puertas de su seno científico para poder estudiar mi carrera profesional. Así como a los diferentes docentes que brindaron sus conocimientos y su apoyo para seguir adelante día a día.

Mi agradecimiento También va dirigido al gerente de la Empresa Desysweb por haberme aceptado a realizar mi tesis en su prestigiosa empresa.

Agradezco también a mi Asesor Mg. Ing. Hernán Ochoa Carbajal, por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento y haberme tenido todo la paciencia del mundo para guiarme durante todo el desarrollo de m tesis.

Y para finalizar, también agradezco a todos los que fueron mi compañeros de clases durante todos los ciclos en la universidad, ya que gracias al compañerismo, amistad y apoyo moral han aportado un alto porcentaje a mis ganas de seguir a delante en mi carrera profesional.

INDICE

Lista de Figuras

Lista de tablas

INTRODUCCIÓN

El presente trabajo de investigación lleva por título “Propuesta de un Plan de Seguridad de la Información basado en la norma ISO 27001 para la empresa Desysweb S.A.C. en el periodo 2017”, para optar el título de Ingeniero de Sistemas, presentado por la bachiller Diana Esther Mascco Tomairo.

El desarrollo avanzado de las tecnologías y comunicaciones, ha sido fundamental para el progreso de la humanidad, trayendo consigo muchos beneficios, pero también amenazas y riesgos que pueden atentar contra los atributos de la seguridad de información (confidencialidad, integridad y disponibilidad).

La información es considerada como un activo importante en las organizaciones. Para la gestión y seguridad de la información, las empresas pueden adoptar alguna de las normas y buenas prácticas existentes en el mercado.

Desysweb es una empresa que provee servicios especializados en tecnología de información (TI), Networking, Telecomunicaciones, Radio-enlaces, WiFi y Redes de Fibra Óptica. Constituida el 11 de enero del 2002, cuenta con presencia en las principales ciudades del país, logrando consolidarse como un socio estratégico de las principales empresas del país.

La empresa Desysweb maneja una cantidad considerable de información en todas las áreas funcionales, cuenta con diversos recursos y equipos pero no son utilizados adecuadamente. Posee pocas políticas de seguridad, métodos y mecanismos que permitan salvaguardar la información;

lo cual es de vital importancia para el éxito y cumplimiento de los objetivos propuestos a corto, mediano y largo plazo.

Como solución a lo descrito líneas arriba, se propone realizar un plan de seguridad de información que permita identificar los activos de información, las amenazas, las vulnerabilidades, las posibles ocurrencias y explotación de las mismas; así poder conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en la empresa, en dónde se establecerán mecanismos alineados a la norma ISO 27001 que ayuden a controlar los riesgos al que se expone la información.

La estructura utilizada en esta investigación se compone de tres capítulos. El Primer Capítulo comprende el planteamiento del problema, justificación y objetivos; el Segundo Capítulo el desarrollo del Marco Teórico y el Tercer Capítulo corresponde al desarrollo del proyecto, y finalmente se termina con la conclusión y recomendación.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

Con el avance que en los últimos años han tenido las tecnologías de información a nivel global, cada día se hace más intensivo el manejo y la manipulación de la información, lo cual ha generado muchos beneficios para la sociedad, es tal que hoy en día muchas organizaciones han incursionado a las nuevas tecnologías de la información mejorando su operatividad y servicio, permitiendo así un desarrollo integral en la sociedad, brindando manejo de información de forma oportuna, creando procesos más eficientes y productivos entre otros, por lo cual se puede decir que es imprescindible la seguridad de la información en los entornos organizacionales.

Desysweb es una empresa que cuenta con compañías socias reconocidas mundialmente en el campo de TI y telecomunicaciones, para ello contamos con ingenieros certificados bajo los más destacados reconocimientos de equipos, telecomunicaciones y fibra óptica. Debido a la considerable cantidad de información que posee la empresa, es necesario considerar medidas para mitigar y evitar posibles riesgos que

puedan llevar a perder uno de los activos más importantes para la organización, la información.

En la empresa Desysweb se puede evidenciar que tienen una red de datos desprotegida en algunas áreas funcionales, carece de planes de contingencia adecuados ante la posible falla o interrupción del sistema, ausencia de mantenimiento y actualización de hardware y software, y cuenta con escasas políticas y métodos para la gestión de copias de seguridad.

La deficiencia en la seguridad física de algunas áreas funcionales ocasiona la posibilidad de robo y/o acceso no autorizado a la información, a su vez, la omisión de capacitación y concientización a la alta dirección y a los colaboradores con respecto a la seguridad de información.

También, está en desarrollo la elaboración de un mini ERP, en dónde por el momento está en operación los módulos de cotizaciones, almacén y proyectos. Éstos cuentan con escasas políticas y mecanismos que ayuden a salvaguardar su integridad, disponibilidad y confidencialidad de la información.

En general, la empresa Desysweb carece de un plan de seguridad de información que le permita optimizar y proteger la integridad de la información que se gestiona diariamente. Es por ello, que se sugiere un plan de seguridad de información para poder identificar los activos de información de la empresa y a su vez a los riesgos, para que sean conocidos, asumidos y gestionados por la organización de una forma

documentada, sistemática, estructurada, repetible y eficiente, a través de la selección de controles.

1.2. Justificación del Proyecto

Existen diversas amenazas, vulnerabilidades y riesgos que pueden atentar contra los atributos de la seguridad de información (confidencialidad, integridad y disponibilidad) que posee la empresa Desysweb. Por ello, se debe tener en cuenta que es muy necesario proteger la información en las áreas funcionales de la empresa; con la ayuda de un plan de seguridad de la información, adecuado a los requisitos y necesidades de la organización.

El plan de seguridad de la información busca mejorar la efectividad en todos los procesos que incursiona y se utiliza la información, tanto en lo administrativo, operativo e incluso tecnológico que se presenta al interior y exterior de la organización, con el fin de mantener el riesgo para nuestra información por debajo del nivel asumible por la propia organización y así optimizar la calidad de los servicios que se prestan a todos los asociados y la sociedad en general, lo cual genera confianza en sus partes interesadas que es fundamental para el crecimiento y la sostenibilidad de la entidad.

También, permite fomentar y extender en toda la organización una cultura apropiada de seguridad de la información, para fortalecer integralmente en cada uno de sus colaboradores, la preservación de los atributos de la seguridad de la información.

Este proyecto permitirá mejorar la imagen de la empresa, debido a que si se llegara a implementar el plan, se generaría un elemento diferenciador como contratista de Claro. Logrando obtener una ventaja competitiva antes las demás contratistas del mercado y a su vez incrementar el nivel de productividad de la organización.

Además, se logrará generar un impacto positivo en las finanzas de la entidad, porque a medida que los colaboradores tengan una conciencia clara de cuál es la información que se debe proteger y gestionar adecuadamente sus riesgos, se puede evitar inversiones innecesarias en seguridad y tecnología de información.

Finalmente, en este proyecto se considera la norma ISO 27001, que es la norma más usada para establecer un idóneo plan de seguridad de información, la cual especifica los requisitos necesarios para establecer y para certificar un SGSI; y la norma ISO 27002, la cual describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendables relacionados con la seguridad.

1.3. Delimitación del Proyecto

1.3.1. Teórica

Comprende realizar un plan de seguridad de información, utilizando la norma ISO 27 0001 para el área de Operaciones de la empresa Desysweb SAC.

1.3.2. Espacial

El desarrollo del presente proyecto se realiza en la empresa Desysweb SAC., ubicada en Av. Esteban Campodónico 474 Urb. Santa Catalina La Victoria – Lima – Perú.

1.3.3. Temporal

Este trabajo tuvo una duración de 3 meses, desde el mes de marzo del 2017 hasta el mes de mayo del 2017.

1.4. Formulación del Problema

¿Cómo ayudará el plan de seguridad de la información basado en la norma ISO 27001 a mitigar los riesgos de la empresa Desysweb?

1.4.1. Problemas específicos

- ¿De qué manera se realizará el inventario de los activos de información de las áreas funcionales de la empresa?
- ¿Qué metodología se usará para la gestión de los riesgos de seguridad de información de los activos de información de la empresa?
- ¿Cuáles son los controles adecuados para lograr mitigar los riesgos de seguridad de información?

1.5. Objetivos

1.5.1. Objetivo General

Proponer un plan de seguridad de la información basado en la norma ISO 27001 para la empresa Desysweb.

1.5.2. Objetivos Específicos

- Identificar y valorar los activos de información.
- Analizar y valorar los riesgos de seguridad de información asociados a los activos de información.
- Evaluar y recomendar los posibles controles adecuados para mitigar los riesgos.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

A lo largo de la investigación bibliográfica, se tomaron como referencia varias tesis que sirvieron de ayuda para el presente trabajo, entre ellas están:

2.1.1. Antecedentes Internacionales

- Guzmán y Taborda (2015), realizó un proyecto titulado ***"Diseño de un sistema de gestión de la seguridad informática– SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá DC"*.**

  En esta investigación se desarrolla un SGSI para empresas del sector textil de las Pymes en las ciudades de Medellín; el diseño se elabora con la norma ISO 27001, la cual provee buenas prácticas apropiadas para el desarrollo e implementación de cada uno de sus componentes.

  Este proyecto contribuyó a poder establecer una metodología de evaluación de riesgos bien definida y a su vez identificar sus elementos.

Se concluye que para la PYME, es importante que protejan sus activos de la información, mediante el diseño de un Sistema de Gestión de Seguridad de Información, para identificar los activos de la empresa, amenazas, vulnerabilidades y riesgos; así se lograría tratar los riesgos e implementar los controles establecidos.

- Guzmán (2015), realizó una tesis titulada ***"Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso"***.

  Las entidades del sector financiero, están en la obligación de garantizar la debida seguridad, protección y privacidad de la información financiera y personal de los usuarios que residen en sus bases de datos, lo que implica, que deben contar con los más altos estándares y niveles de seguridad con el propósito de asegurar la debida recolección, almacenamiento, tratamiento y uso de esta información. Por eso, se busca diseñar un Sistema de Gestión de Seguridad de la Información para una entidad financiera de segundo piso, teniendo en cuenta para esto el marco de referencia de la norma ISO 27001:2013

  Este proyecto aportó a la identificación de las actividades más relevantes de la fase de planificación de la ISO 27001.

  Se llega a la conclusión que la ISO/IEC 27001:2013 es una herramienta de gran ayuda que permite identificar los diferentes

aspectos de las organizaciones para establecer un modelo de seguridad de la información. Además es necesario establecer políticas de seguridad que ayuden a la organización a mitigar los riesgos, y también contar con el apoyo de la alta dirección.

- Palacios (2015), realizó un proyecto titulado ***"Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la norma ISO 27001: 2013"***.

  Este trabajo sirvió como guía en la metodología de evaluación de riesgos, para poder realizar correctamente la identificación de los activos de información, y así poder reconocer sus respectivos elementos (amenazas, vulnerabilidades e impacto). Se concluye que para realizar el diseño del SGSI, se debe contar con el apoyo de la alta dirección. También realizar un correcto levantamiento de los activos de información, así determinar sus respectivas amenazas y vulnerabilidades, de esta forma identificar y analizar los riesgos, ocurrencia e impacto de los eventos negativos que pueden atentar contra la seguridad de la información, lo cual permite proporcionar controles para prepararse o prevenir dichos eventos.

2.1.2. Antecedentes Nacionales

- En el trabajo de Barrantes y Herrera (2012), titulado **"Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos"**, se presenta una investigación que surge de la necesidad que tiene la empresa

Card Perú S.A. de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; todo ello, se logró realizar con la ayuda de un Sistema de Gestión de Seguridad de Información.

Este proyecto sirve como guía para evidenciar y aportar el conocimiento necesario en diseño de SGSI, así poder establecer la metodología de evaluación de riesgos.

Este trabajo concluye que diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.

- Espinoza (2013), realizó una tesis titulada ***"Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001: 2005 para una empresa de producción y comercialización de productos de consumo masivo"***.

  Este proyecto abarca solamente el análisis y diseño del SGSI, basado en la norma ISO/IEC 27001:2005 y está dirigido a procesos, activos, riesgos, y demás consideraciones, de una empresa de producción y comercialización de productos de consumo masivo.

  Este proyecto contribuyó al uso de técnicas necesarias para el levantamiento de los activos de información y el análisis de

riesgos, que permitan la adecuada definición de controles en base a los hallazgos encontrados.

Este trabajo concluye que la adecuada gestión de la seguridad de información es algo que debe estar ya incluido en la cultura organizacional de las empresas y se debe concientizar a los colaboradores de dicha empresa, sobre la seguridad de la información y su importancia, y realizar evaluaciones periódicas a los indicadores de seguridad de la empresa y de los riesgos encontrados.

- Ampuero (2011), realizó un proyecto titulado ***"Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros"***.

  Este trabajo ayudó al reconocimiento de la importancia que tiene el apoyo de la alta dirección para el avance del proyecto y también ayudó como guía en la identificación de los activos, amenazas, vulnerabilidades, riesgos y controles.

  Se concluye que para realizar el diseño del SGSI, es necesario saber identificar los activos de la información, a su vez identificar sus respectivas amenazas y vulnerabilidades, calcular el impacto de los riesgos en la compañía de seguros y poder formular los controles correctos para mitigar los riesgos. Además de nada sirve lo mencionado anteriormente, sino se cuenta con el apoyo de la alta dirección.

2.2. Bases teóricas

2.2.1. Sistema de Gestión de Seguridad de Información (SGSI)

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Martelo, Madera y Betín (2015), define que un Sistema de Gestión de Seguridad de Información es un conjunto de políticas que establece la alta dirección con el propósito de definir, construir, desarrollar y mantener la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa.

Según ISO (2017), el propósito de un sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

2.2.1.1. Beneficios de SGSI para las organizaciones

Según Cortés y Ardela (2012), indica que los beneficios de un SGSI para las organizaciones son los siguientes:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan continuamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.

2.2.1.2. Actividades relevantes de un SGSI

Según Cortés y Ardela (2012), indica que las actividades relevantes de un SGSI son los siguientes:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.

- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

2.2.2. Estándares de Seguridad de Información

Entre los estándares más conocidos tenemos la Familia ISO 27001 y COBIT.

2.2.2.1. ISO y la familia 27000

Según ISO (2017), ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

2.2.2.2. COBIT

Según ISACA (2017), COBIT fue lanzado por primera vez en 1996 y se actualiza continuamente para satisfacer las necesidades actuales y seguir siendo relevantes. Ahora en la versión 5, COBIT es un marco integral de prácticas, herramientas analíticas y modelos globalmente aceptados que pueden ayudar a cualquier empresa a abordar con eficacia las cuestiones empresariales a través de la gobernanza y la gestión de la información y la tecnología.

2.2.3. Familia ISO 27000

2.2.3.1. ISO 27000

La ISO 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. La norma ISO 27000 se encuentra en fase de desarrollo, contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma es gratuita, a diferencia de las demás de la serie, que tienen un coste. (Cabrales, 2016)

2.2.3.2. ISO 27001

Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma mediante la cual el SGSI de una organización es evaluado para lograr su certificación por auditores externos. Dado que ésta fue la sustitución de la BS 7799-2, se establecieron condiciones para realizar la transición de aquellas empresas certificadas en ésta última. En su Anexo A, lista en forma de resumen los objetivos de control y controles que desarrolla la ISO/IEC 17799:2005 (actualmente ISO/IEC 27002:2005), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de

no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. (Pantaleone y Silva, 2013)

Wu fu (2016), indica que la norma ISO 27001 contiene:

- Introducción: generalidades e introducción al método PDCA.
- Objeto y campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- Normas para consulta: otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- Auditorías internas del SGSI: cómo realizar las auditorías internas de control y cumplimiento.

- Revisión del SGSI por la dirección: cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- Mejora del SGSI: mejora continua, acciones correctivas y acciones preventivas.
- Objetivos de control y controles: anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
- Relación con los Principios de la OCDE: anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
- Correspondencia con otras normas: anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.
- Bibliografía: normas y publicaciones de referencia.

2.2.3.3. ISO 27002

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Está hecha en base a la norma BS 7799-1 e ISO/IEC 17799:2005. La norma ISO/IEC 27001:2005 contiene un anexo que resume los controles de ISO/IEC 17799:2005, a diferencia que en la primera los requerimientos son

específicos y obligatorios para la organización que desee certificar. (Pantaleone y Silva, 2013)

Cordero (Cordero, 2015), indica que la norma ISO 27002 contiene:

- Introducción: conceptos generales de seguridad de la información y SGSI.
- Campo de aplicación: se especifica el objetivo de la norma.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Estructura del estándar: descripción de la estructura de la norma.
- Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Política de seguridad: documento de política de seguridad y su gestión.
- Aspectos organizativos de la seguridad de la información: organización interna; terceros.
- Gestión de activos: responsabilidad sobre los activos; clasificación de la información.
- Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

- Seguridad física y ambiental: áreas seguras; seguridad de los equipos.
- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.
- Bibliografía: normas y publicaciones de referencia.

2.2.3.4. ISO 27003

En fase de desarrollo; su fecha prevista de publicación fue mayo de 2009. Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. (Aguirre y Zambrano, 2015)

2.2.3.5. ISO 27004

En fase de desarrollo; su fecha prevista de publicación fue noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia

de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA. (Chacón, 2012)

2.2.3.6. ISO 27005

Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

2.2.3.7. ISO 27006

Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y

certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSI. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. (Córdoba, 2015)

2.2.3.8. ISO 27007

En fase de desarrollo; su fecha prevista de publicación fue Mayo de 2010. Consiste en una guía de auditoría de un SGSI.

2.2.3.9. ISO 27011

En fase de desarrollo; su fecha prevista de publicación fue finales de 2008. Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

2.2.4. Ciclo De Deming

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la

calidad. En la figura 2-1, detalla las actividades del ciclo de mejora continua del SGSI:

- **P**lan (planificar): establecer el SGSI.
- **D**o (hacer): implementar y utilizar el SGSI.
- **C**heck (verificar): monitorizar y revisar el SGSI.
- **A**ct (actuar): mantener y mejorar el SGSI.

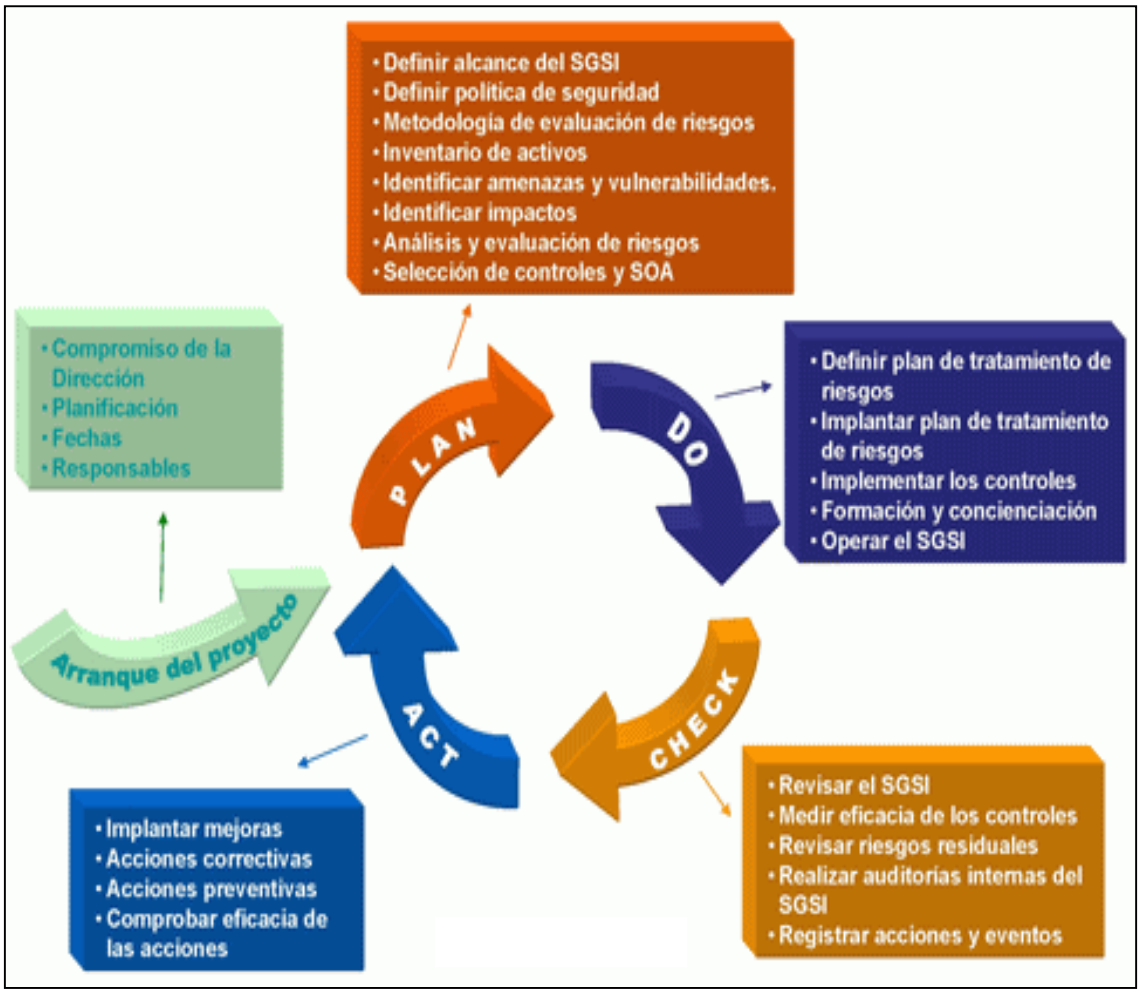


Figura 2-1 Ciclo de mejora continua del SGSI.
Fuente: http://www.iso27000.es/sgsi.html

Según ISO (2017), las actividades de las fases del ciclo de Deming son las siguientes:

2.2.4.1. Planeamiento

En la fase de planeamiento se realiza las siguientes actividades:

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
- Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes...) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, etc.
- La política del SGSI es normalmente un documento muy general, una especie de "declaración de intenciones" de la Dirección pero que incluya el marco

general y los objetivos de seguridad de la información de la organización; tenga en cuenta los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información; esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI; establezca los criterios con los que se va a evaluar el riesgo; y esté aprobada por la dirección.

- Definir el enfoque de evaluación de riesgos mediante una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio. El riesgo nunca es totalmente eliminable, por lo que es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar grados de subjetividad que falseen la valoración de los riesgos. Existen numerosas metodologías estandarizadas para la evaluación de riesgos y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia. ISO 27001:2005 no impone ninguna para que cada organización pueda aplicar la que estime más oportuno

y funcional según el esfuerzo de análisis y recursos que pueda aplicar.

- Identificar los riesgos:
- Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
- Identificar las amenazas relevantes asociadas a los activos identificados;
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
- identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

- Analizar y evaluar los riesgos:
- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
- Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
- Estimar los niveles de riesgo;

- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
- Aplicar controles adecuados (mitigación);
- Aceptar el riesgo (de forma consciente), siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
- transferir el riesgo total o parcialmente a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.
- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001:2005 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI. Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación final en cada revisión y/o acciones de tratamiento. El riesgo residual es el que queda, aún después de haber

aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

- Definir una declaración de aplicabilidad también llamada SOA (Statement of Applicability) que incluya:
  - Los objetivos de control y controles seleccionados y los motivos para su elección;
  - Los objetivos de control y controles que actualmente ya están implantados;
  - Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

2.2.4.2. Implementación

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

2.2.4.3. Monitoreo y revisión

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  - Identificar brechas e incidentes de seguridad;
  - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos

tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;

- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

• Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

• Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

2.2.4.4. Mantener y mejorar

La organización deberá regularmente:

• Implantar en el SGSI las mejoras identificadas.

• Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan

• Solucionar no conformidades detectadas y materializadas. En relación a la cláusula 8 de ISO 27001:2005 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.
- PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.

2.2.5. Metodología de Gestión de Riesgos

El proceso de gestión de riesgos involucra cuatro actividades cíclicas:

- La identificación de activos y los riesgos a los que están expuestos.
- El análisis de los riesgos identificados para cada activo.
- La selección e implantación de controles que reduzcan los riesgos.
- El seguimiento, medición y mejora de las medidas implementadas.

2.2.5.1. MAGERIT II

Según Fernández (2003), MAGERIT II es una metodología para administrar riesgos, que tiene como uno de sus principales objetivos, el ofrecer un método para analizar los riesgos y ayudar a descubrir y planificar las

medidas oportunas para mantener los riesgos bajo control.

2.2.5.2. ISO 27005

Consiste en una guía para la gestión del riesgo de la seguridad de la información y es un apoyo para la ISO/IEC 27001 y la implementación de un SGSI.

2.2.5.3. NIST SP 800-30

Guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos. La guía provee apoyo en los procesos de valoración y mitigación dentro de la gestión de riesgos. (Castro y Bayona, 2011)

2.2.5.4. UNE 71504

Es una metodología de análisis y gestión de riesgos para los sistemas de información. Desarrollada por el comité técnico AEN/CTN 71 Tecnología de la información de AENOR. Se compone de 4 fases:

- Método de análisis
    - Tareas preparatorias
    - Caracterización de activos
    - Caracterización de las amenazas
    - Cálculo del riesgo potencial
    - Cálculo de las salvaguardas
    - Cálculo del riesgo residual
- Evaluación de riesgos

- Tratamiento de riesgos
- Administración de la gestión de riesgos

2.2.5.5. OCTAVE

Según SEI (2017), OCTAVE es una metodología de evaluación de riesgos flexible y autodirigida. Un pequeño equipo de personas de las unidades operativas (o de negocios) y el departamento de TI trabajan juntos para atender las necesidades de seguridad de la organización. El equipo se basa en el conocimiento de muchos empleados para definir el estado actual de la seguridad, identificar los riesgos de los activos críticos y establecer una estrategia de seguridad. Se puede adaptar para la mayoría de las organizaciones.

El método OCTAVE se basa en ocho procesos que se dividen en tres fases. En las organizaciones de educación superior, suele ir precedida de una fase exploratoria (conocida como Fase Cero) para determinar los criterios que se utilizarán durante la aplicación del método de OCTAVE.

Las tres fases de OCTAVE son:

- Fase 1

  Desarrollar estrategias de seguridad iniciales.

- Fase 2: Visión tecnológica

  Identificar las vulnerabilidades de la infraestructura.

- Fase 3: Análisis de riesgos

  Desarrollar estrategias y planes de seguridad.

2.2.5.6. CRAMM

Cordero (2015), indica que CRAMM es una metodología para el análisis y gestión de riesgo, que permite: Definir un marco de gestión del riesgo, identificar riesgos, identificar loa propietarios de los riesgos, evaluar riesgos, definir niveles aceptables de riesgo, identificar respuestas adecuadas al riesgo, implantar respuestas, obtener garantías de la efectividad, monitorizar y revisar.

2.2.5.7. MEHARI

Patrocinado por la organización CLUSIF, con el fin de ayudar a ejecutivos en sus esfuerzos para gestionar la seguridad de información y los recursos de TI para reducir los riesgos asociados.

2.2.6. Propuesta de la Metodología para el plan de seguridad de la información

Identificaremos la propuesta del Modelo del plan de seguridad de la información para una empresa de telecomunicaciones como Modelo PSI-DSW para referirnos de manera corta y precisa. A continuación, se describen las actividades que se realizarán para el PSI-DSW.

El modelo que se propone para el plan de un Sistema de Seguridad de Información para la empresa Desysweb debe realizarse en 2 etapas según se indica en la Tabla 3-1.

Tabla 2-1 Etapas del PSI-DSW

Etapas	Descripción
Etapa 0	Diagnóstico según las normas elegidas.
Etapa 1: Diseño del PSI-DSW	Definir alcance del PSI-DSW
	Definir objetivo de seguridad
	Inventario de activos
	Valoración de los activos
	Listado de amenazas
	Listado de vulnerabilidades
	Valoración de los riesgos
	Identificar impactos
	Selección de controles
	Definir política de seguridad

Figura 2-2 Etapas del Modelo PSI-DSW
Fuente: Elaboración Propia

2.2.6.1. La Etapa 0: Diagnóstico según las normas elegidas.

Para conocer el grado de conocimiento en seguridad de la información en la empresa Desysweb, se aplicó un cuestionario a los socios de la empresa y al administrador de redes y seguridad sobre los procesos, controles y en general la cultura en seguridad de la información en la organización.

2.2.6.2. La Etapa 1: Diseño del PSI-DSW.

La Etapa 1 comprende el diseño del PSI-DSW y abarcará básicamente cuatro aspectos cruciales para el desarrollo del proyecto. Estos aspectos son:

- Determinación del alcance del proyecto
- Definición de los objetivos de seguridad.
- Definición de las políticas de seguridad.
- Metodología de evaluación y análisis de riesgo.

2.2.6.3. Determinación del alcance del PSI-DSW

El alcance se documenta en términos de los servicios que ofrecen la empresa, los activos, la tecnología y procesos de las áreas funcionales. Se utilizará una tabla de prioridades que contemple las prioridades para los aspectos antes mencionados y cuya información se obtuvieron mediante cuestionarios.

2.2.6.4. Definición de los objetivos de seguridad.

Los objetivos de seguridad se realizan en base a los propósitos u objetivos de la organización.

2.2.6.5. Metodología de evaluación y análisis de riesgo

Una vez establecido el alcance y definidos los objetivos de seguridad materializados en el documento sobre la política de seguridad de la información, la siguiente actividad es la realización de la metodología de evaluación de riesgos.

- **Identificación de activos de la Información**

  Se identifican a los activos de la información del área determinada en el alcance del PSI-DSW, también a los propietarios funcionales para todos los activos importantes. También los activos de información en grupos de activos de información, ello se muestra en la Tabla 2-2 y la Tabla 2-3.

Tabla 2-2 Tabla de activos de información y propietarios funcionales

Nº	Activo de información	Propietario funcional

Fuente: Elaboración Propia

Tabla 2-3 Clasificación de los activos de información

Grupos de activos de Información	Activos de Información

Fuente: Elaboración Propia

- **Valoración de Activos de Información**

  La valoración es el atributo que hace valioso a un activo de información en términos de su importancia para la empresa Desysweb. Mediante su

dimensionamiento permite valorar las consecuencias de la materialización de una amenaza. Para valorar los activos de información se emplea una escala cualitativa mostrada en la Tabla 2-4.

Tabla 2-4 Valoración de los activos de información

Valor		Criterio
MA	Muy Alto	Daño muy grave a la empresa
A	Alto	Daño grave a la empresa
M	Mediano	Daño importante en la empresa
B	Bajo	Daño menor a la empresa
MB	Muy bajo	Sin importancia

Fuente: Elaboración Propia

En la Tabla 2-5 siguiente se permite evaluar los activos de información mediante su relación a los conceptos claves de información: Confidencialidad, Integridad y Disponibilidad.

Tabla 2-5 Evaluación de los activos de información

Nº	Activo de Información	Confidencialidad	Integridad	Disponibilidad	Total

Fuente: Elaboración Propia

- **Identificación de Amenazas**

  Se realiza un listado de amenazas consideradas vitales y un listado de funciones organizacionales mostrando su dependencia con determinados recursos, en la tabla 2-6, las amenazas que afectan los

activos de información, se ha agrupado los activos según su funcionalidad.

Tabla 2-6 Identificación de amenazas a los activos de información

Nº	Grupos de activos de la Información	Amenazas

Fuente: Elaboración Propia

- **Posibilidad de ocurrencia de amenazas**

  A cada amenaza identificada se ha calculado la posibilidad de ocurrencia y el impacto que puede ocasionar en la empresa Desysweb. Lo anterior se muestra en la Tabla 2-7.

Tabla 2-7 Valoración de ocurrencias de amenazas

Valor		Criterio
A	Alto	Daño grave a la empresa
M	Mediano	Daño importante a la empresa
B	Bajo	Daño menor a la empresa

Fuente: Elaboración Propia

La organización tomará decisiones sobre las opciones de tratamiento del riesgo además determinará que amenazas se reducirán con controles, cuáles se aceptarán y con cuáles convivir, cuáles se transferirán y cuales se evitarán. En la tabla 2-8, se muestra el listado de amenazas y su posible ocurrencia:

Tabla 2-8 Listado de amenazas y la posibilidad de ocurrencia

Nº	Grupos de activos de información	Amenazas	Posibilidad de ocurrencia

Fuente: Elaboración Propia

- **Identificación de vulnerabilidades (debilidades)**

  Una vez identificadas las distintas vulnerabilidades por cada amenaza, se define el grado en que la amenaza puede explotar cada vulnerabilidad. Lo anterior, se muestra en tabla 2-9:

Tabla 2-9 Vulnerabilidad de los activos de información

Nº	Grupos de activos de información	Vulnerabilidades

Fuente: Elaboración Propia

- **Valoración de vulnerabilidad**

  En la tabla 2-10 se muestran los criterios que se tomarán en cuenta para la valoración de la vulnerabilidad.

Tabla 2-10 Tabla de valoración de la vulnerabilidad

Valor		Criterio
A	Alto	Vulnerabilidad muy deficiente
M	Mediano	Vulnerabilidad deficiente
B	Bajo	Vulnerabilidad controlada

Fuente: Elaboración Propia

Alto: Permite a un atacante remoto violar la protección de seguridad del sistema Permite a un atacante local tomar control completo del sistema

Mediano: Permite a un atacante remoto o local violar la protección de seguridad. No toma control completo del sistema.

Bajo: La vulnerabilidad no permite obtener información valiosa de por sí ni control del sistema, si no que da al

atacante información que le puede ayudar a encontrar otras vulnerabilidades en el sistema. La vulnerabilidad resulta inocua

En la Tabla 2-11, se muestra los grupos de activos de información, sus respectivas vulnerabilidades y la posibilidad de ocurrencia de las vulnerabilidades.

Tabla 2-11 Posible evaluación de las vulnerabilidades

Nº	Grupos de activos de información	Vulnerabilidad	Posibilidad de explotación

Fuente: Elaboración Propia

- **Estimación del Valor de los Activos en Riesgo**

  La Tabla 2-12 se muestra la evaluación del riesgo, a fin de determinar el daño cualitativo que el riesgo pudiera causar a los activos de información.

Tabla 2-12 Evaluación del riesgo

Nº	Grupos de activos de información	Amenazas	Posibilidad de ocurrencia	Posibilidad de explotación	Valor activo de información

Fuente: Elaboración Propia

- **Posibilidad de Ocurrencia del Riesgo**

  En la tabla 2-13, se muestra la posibilidad de ocurrencia del riesgo se obtiene analizando cada activo de información, con referencia a las amenazas que sufre y la posibilidad que ocurra, así como sus vulnerabilidades y la posibilidad que tiene de ser explotadas.

Tabla 2-13 Posibilidad de ocurrencia del riesgo

Nº	Grupos de activos de información	Amenazas	Vulnerabilidad	Valor activo de información	Posibilidad de ocurrencia

Fuente: Elaboración Propia

- **Valor del Riesgo de los Activos.**

  El Impacto hace referencia a la magnitud de las consecuencias, que tiene para la empresa Desysweb. el hecho de que uno o varios activos de información hayan visto comprometido su confidencialidad, integridad o disponibilidad debido a que una o varias amenazas en las que se hayan explotado sus vulnerabilidades. Al estimar un determinado nivel de impacto es necesario considerar la criticidad de los activos de información afectados. La exposición al riesgo, también es evaluada desde un análisis cuantitativo y cualitativo del riesgo.

- **Análisis cuantitativo:** Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en cifras concretas de forma objetiva.
- **Análisis cualitativo:** Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en términos subjetivos (Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo). En la tabla 2-

14 y tabla 2-15, se muestra las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores. En la tabla 2-16, se muestra la valoración de las amenazas según su impacto y probabilidad.

Tabla 2-14 Valoración de la probabilidad de ocurrencia

	Valor		Criterio
5	MA	Probable	Posibilidad de incidentes repetitivos
4	A	Posible	Posibilidad de incidentes aislados
3	M	Poco probable	Posibilidad de ocurrencia muy moderada
2	B	Raro	No es probable que ocurra
1	MB	Imperceptible	Posibilidad de ocurrencia muy escasa

Fuente: Elaboración Propia

Tabla 2-15 Valoración del impacto

	Valor		Criterio
5	MA	Catastrófico	Deficiencia detectada, implica cambios en los procedimientos para su corrección (reingeniería de procesos).
4	A	Significativo	Deficiencia detectada, implica más de un procedimiento para su corrección
3	M	Moderado	Deficiencia detectada, implica un procedimiento para su corrección.
2	B	Menor	Riesgo controlado el cual revierte la mínima complicación posible para el sistema de información, el cual no requiere ninguna contingencia.
1	Mb	Insignificante	Este punto se obtiene como producto de la revisión y verificación de las actividades, que resultado tienen luego de ser ejecutadas, si el resultado es satisfactorio o de pleno cumplimiento.

Fuente: Elaboración Propia

Tabla 2-16 Valoración del riesgo

Nº	Amenazas	Probabilidad de ocurrencia	Impacto

Fuente: Elaboración Propia

- **Mapa de calor**

  El mapa de calor permite representar de forma gráfica un plano conformado por la ubicación los riesgos de acuerdo a su probabilidad y su impacto.

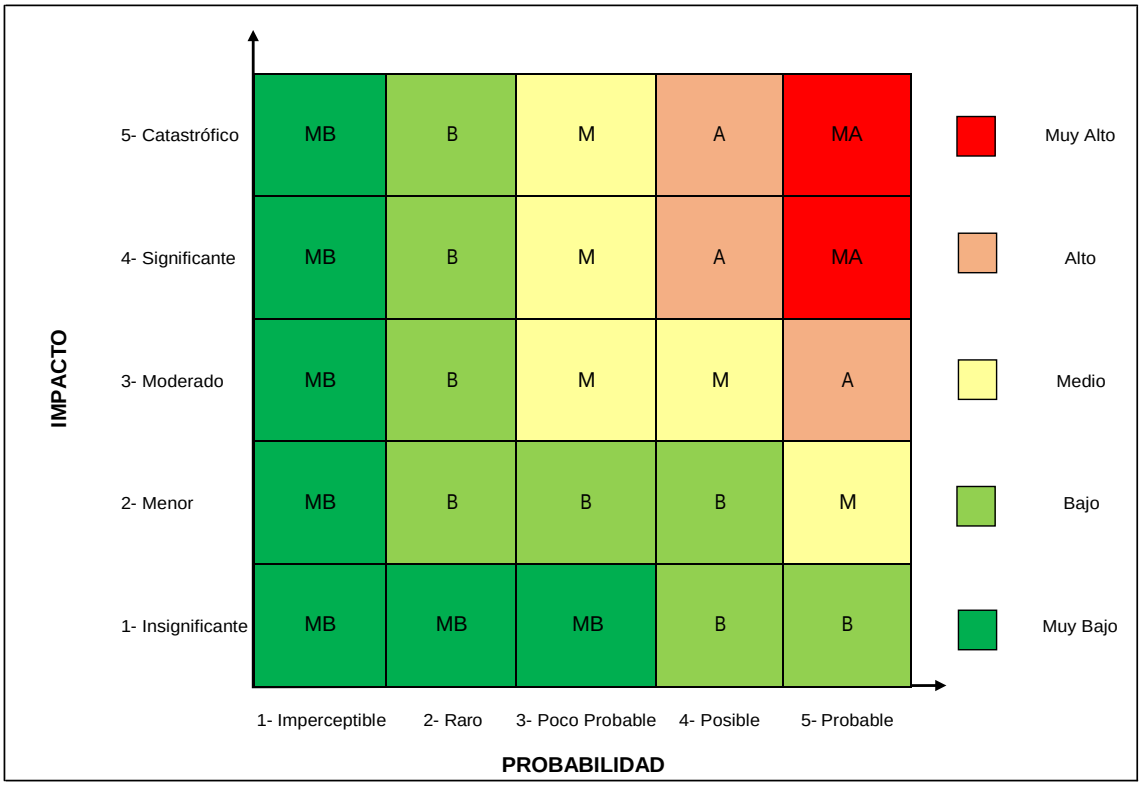


Figura 2-3 Mapa de calor
Fuente: Elaboración Propia

De acuerdo al mapa de calor, en la tabla 2-17 se identifica el nivel de los riesgos (probabilidad x impacto)

Tabla 2-17: Niveles del riesgo

Nº	Amenazas	Probabilidad de ocurrencia	Impacto	Nivel del riesgo

Fuente: Elaboración Propia

- **Tratamiento de riesgos**

  Se va a identificar y evaluar las distintas opciones de tratamiento de los riesgos.

- Mitigar: aplicar controles adecuados
- Aceptar el riesgo: siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos
- Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan.
- Transferir el riesgo total o parcialmente a terceros.

  En la tabla 2-18, se muestra las opciones de tratamiento (mitigar, aceptar, evitar y transferir) para cada riesgo identificado.

Tabla 2-18 Opciones de tratamiento del riesgo

Nº	Amenazas	Probabilidad de ocurrencia	Impacto	Nivel del riesgo	Opción de tratamiento

Fuente: Elaboración Propia

- **Selección de controles**

  De acuerdo a los requerimientos de seguridad, se han de identificar controles que garanticen que los riesgos sean reducidos a un nivel aceptable.

  En la tabla 2-19, se muestra los objetivos de control con sus respectivas salvaguardas para cada amenaza identificada.

Tabla 2-19: Selección de controles

Nº	Amenazas	Nivel del riesgo	Opción de tratamiento	Objetivos de control	Control	Tratamiento

Fuente: Elaboración Propia

2.2.6.6. Definición de las políticas de seguridad.

Luego de haber terminado con el análisis y gestión de riesgos, para completar el diseño del PSI-DSW, se plantean algunas políticas de seguridad para garantizar el buen funcionamiento del PSI-DSW.

Esta etapa se establece una orientación general sobre las directrices y principios de actuación en relación con la seguridad de la información de la empresa Desysweb.

2.3. Marco Conceptual

2.3.1. Información

Se define a la información como conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que esté guardada o sea transmitida, de su origen o de la fecha de elaboración.

Según Espinoza (2013), los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, necesarios para que la organización funcione y alcance los objetivos que propone su dirección.

Se considera al activo de información como algo a lo que una organización asigna un valor y le genera valor para la misma, por lo que la organización debe proteger.

2.3.2. Seguridad de Información

La seguridad de la información, según ISO (2017) consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

2.3.3. Atributos de la Seguridad de información

La información tiene varios atributos, pero la seguridad de información se caracteriza por tres atributos:

- Confidencialidad: Se refiere a que la información debe estar a disposición de personal autorizado.
- Integridad: Se refiere a que la información debe mantenerse de forma exacta y completa.

- Disponibilidad: Se refiere a que la información debe ser accedida y utilizada por personal autorizado en el momento requerido.

2.3.4. Amenaza

Las amenazas son algo que puede potencialmente causar daño a los activos de información. Las amenazas pueden ser de distintos tipos con base en su origen. Las amenazas se pueden clasificar en (Alexander, 2007):

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (crisis financieras, perdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

2.3.5. Vulnerabilidad

Las vulnerabilidades son las debilidades de la organización que pueden ser explotados por una amenaza. Según García y Alegre (2011), las vulnerabilidades pueden clasificarse en las siguientes categorías:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, empleados desmotivados, etc.).
- Control de acceso (Segregación inapropiada de redes, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, contraseña sin modificarse, etc.).
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, mal cuidado de equipos, etc.).
- Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, falta de protección en redes públicas de conexión, etc.).
- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, etc.).

2.3.6. Riesgo

El riesgo es la posibilidad o probabilidad que una amenaza explote una vulnerabilidad en los activos causando daños o pérdidas, de esta manera se perdería los atributos de la seguridad de información (confidencialidad, disponibilidad e integridad).

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia. En la Figura 2-4, se muestra la interrelación entre los activos, amenazas, vulnerabilidades, riesgos, impacto y controles.

Figura 2-4 Interrelación de los elementos de los riesgos.
Fuente: http://www.iso27000.es/sgsi.html

2.3.7. Gestión de Riesgos

Según ISO (2017), la gestión de riesgo es un enfoque estructurado para manejar la incertidumbre, es decir la posibilidad de que ocurra o no un riesgo, para evitar que ocurran

consecuencias no deseadas dado el caso que el riesgo se haga realidad, para ello se pueden llevar a cabo una secuencia de actividades para evaluar el riesgo, mitigar el riesgo y estrategias para manejar el riesgo que incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular de tal forma que las posibles pérdidas y la posibilidad que se haga presente el riesgo se minimicen.

2.3.8. Riesgo residual

Es el riesgo que encontramos una vez ha disminuido el riesgo tras aplicar medidas correctivas, bien sean aplicadas realmente o mediante un proceso de simulación.

2.3.9. Impacto

El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza. De forma dinámica, es la diferencia en las estimaciones del estado de seguridad del activo antes y después de la materialización de la amenaza sobre éste. (Fernández, 2003)

2.3.10. Política de seguridad

Según Navarro, Díaz y Marín (2011) definen que las políticas de seguridad son las directrices y objetivos generales de una empresa relativos a la seguridad, expresados formalmente por la dirección general. La Política de seguridad de una empresa es un documento auditable ya sea por los auditores internos de la

empresa o por externos en busca de una certificación, inclusive por el cliente. Por este motivo este documento debe ser entendido a todos los niveles, desde el personal operativo / operador hasta los altos mandos (directores, gerentes, etc.)

2.3.11. Controles

Según Valencia (2013), refiere que los controles son como el medio para manejar el riesgo, incluidas las políticas, los procedimientos, las orientaciones, las prácticas o estructuras organizacionales usada como salvaguarda o medida preventiva.

CAPÍTULO III: DISEÑO DEL PLAN DE SEGURIDAD DE INFORMACIÓN

3.1. METODOLOGÍA DE PLAN DE SEGURIDAD DE INFORMACIÓN

Identificaremos la propuesta del plan de seguridad de la información para una empresa de telecomunicaciones como PSI-DSW para referirnos de manera corta y precisa.

3.1.1. Estructura organizativa de la empresa Desysweb

La estructura organizativa de la empresa Desysweb cuenta con las siguientes áreas:

Directorio: compuesta por tres socios patrocinadores, son aquellos que financian a la empresa.

Gerencia General: Se encarga de la toma de decisiones, mantener a la organización, establecer y cumplir los objetivos alineados con la misión y visión de la empresa.

Área de Operaciones: Comprende sub áreas de planta Interna, proyectos especiales, mantenimiento (preventivo y correctivo), administración de redes e ingeniería y desarrollo.

Área de Documentación y Liquidación: Comprende la documentación de las distintas sub área de operaciones y la liquidación de los gastos correspondientes por los trabajos realizados.

Área de Logística: Es el área responsable de coordinar las diferentes áreas de almacén, optimizar la política de aprovisionamiento y distribución de la empresa, etc.

Área de Recursos Humanos: Es el área encargada de la dirección eficiente y efectiva del recurso humano de la empresa, el reclutamiento y selección de personal capaz, responsable y adecuado a los puestos de la empresa, la motivación, capacitación y evaluación del personal; el establecimiento de un clima laboral agradable para el desarrollo de las actividades.

Área de Finanzas: Es el área que se encarga del optimo control, manejo de recursos económicos y financieros de la empresa, esto incluye la obtención de recursos financieros tanto internos como externos, necesarios para alcanzar los objetivos y metas empresariales y al mismo tiempo velar por que los recursos externos requeridos por la empresa sean adquiridos a plazos e intereses favorables.

Área Comercial: Es el área que se encarga de canalizar los servicios que se ofrecen a los clientes, también de la investigación de mercados, la determinación del precio de los servicios la publicidad y la promoción.

Con esta estructura organizacional se puede formular un Modelo de PSI-DSW flexible y particular para la empresa Desysweb. En el Anexo A, se presenta el organigrama de la empresa Desysweb.

3.1.2. Etapas del PSI-DSW

El modelo propuesto establece que se debe realizar el planeamiento y la implementación por etapas, y después de implementar las etapas, se debe realizar un proceso de mejora continua haciendo la revisión y mejora de las etapas anteriores. En este proyecto solamente se abarcará la etapa preliminar y la etapa de planeamiento.

3.2. PLANEAMIENTO DEL PSI-DSW

3.2.1. Diagnóstico

Para conocer el grado de conocimiento en seguridad de la información en la empresa Desysweb, se aplicó un cuestionario a los socios de la empresa y al administrador de redes y seguridad, sobre los procesos, controles y en general la cultura en seguridad de la información en la organización. En el Anexo B, se presenta los respectivos cuestionarios.

De los cuestionarios, se puede evidenciar que la organización cuenta con políticas como por ejemplo:

- Se realiza el backup de correo y de firewall interdiario, y el servidor en la nube cada semana.

- Los nombres de usuario y contraseña secreta que son asignadas para el acceso a los sistemas, aplicaciones, y los recursos de la empresa, son personales, intransferibles y estrictamente confidenciales.
- La infraestructura de sistemas, aplicaciones y los recursos de la empresa deben ser utilizados únicamente para los fines laborales.
- La política de contraseñas es cambiarla mensualmente, especialmente la del correo corporativo y el cambio es mensual para evitar el phishing.

El resto de políticas están en el Anexo B, pero de lo anterior, se analizó la realidad de la empresa y en muchos casos particulares no se cumple con las políticas establecidas. Además no se cuida ni se protegen los activos de información, carecen de valor en la organización. No se tiene mucho conocimiento en los conceptos de seguridad de información; es por ello que la empresa Desysweb necesita diseñar el PSI-DSW para sus áreas funcionales y así poder mejorar los procesos de la empresa.

3.2.2. Alcance del PSI-DSW

Para definir y formalizar el alcance del PSI-DSW, se tiene en cuenta los servicios que ofrecen la empresa, los activos, la tecnología y procesos de las áreas funcionales. Para ello, se elaboró la tabla 3-1 que contempla las prioridades de los aspectos antes mencionados y cuya información se obtuvieron mediante entrevistas a los socios de la empresa y al administrador de redes

e informática. En dichos cuestionarios se tomó en cuenta una escala del 1 al 5, de acuerdo al nivel de importancia que tienen estas categorías (dónde 1, indica que tiene menor importancia y 5, equivale a una mayor importancia) en las áreas funcionales de la empresa Desysweb SAC.

Tabla 3-1 Áreas funcionales que definen en alcance del PSI-DSW

N	Área	Servicios	Proceso	Activos	Tecnología	Total
1	Operaciones	5	4	5	5	19
2	Documentación y Liquidación	3	4	4	4	15
3	Logística	4	4	4	3	15
4	Finanzas	2	3	4	3	12
5	Recursos Humanos	2	3	3	2	10
6	Comercial	2	2	2	2	8

Además, en el Anexo C, se evidencia un compromiso de la Empresa Desysweb; dónde en dicho documento se manifiestan la misión, visión, servicios que ofrece la empresa y también hace hincapié a que el área más importante para la empresa es la de Operaciones, porque genera más productividad a la empresa.

También en el Anexo D, se detallan los procesos, activos y tecnología que son parte de las sub áreas Mantenimiento, Instalaciones y Proyectos.

De lo anterior, el alcance del PSI-DSW, abarca solo para el área funcional de Operaciones, que involucra las sub áreas de proyectos, instalaciones y mantenimiento.

3.2.3. Objetivos del PSI-DSW

Los objetivos del PSI-DSW son los siguientes:

- Formalizar La “Cultura de la Seguridad de la Información” en la empresa Desysweb, estableciendo los procesos internos encargados de garantizar la seguridad de la información, es decir, proteger la confidencialidad, integridad y disponibilidad de la misma.
- La toma de conciencia en materia de seguridad de todo el personal dependiente de la empresa.
- La vigilancia del cumplimiento de la legislación vigente en materia de seguridad de la información y protección de datos de carácter personal.
- La documentación, formalización y registro de los procedimientos relacionados con la seguridad de la información.
- Cumplir con los requerimientos legales y reglamentarios aplicables a la empresa y al Sistema de Gestión de Seguridad de la Información.
- Garantizar el acceso a la información de acuerdo con los niveles de la organización y criterios de seguridad que

establezca la empresa, la normatividad aplicable y/o las partes interesadas.

- Mantener la integridad de la información de la empresa, teniendo en cuenta los requisitos de seguridad aplicables y los resultados de la valoración y el tratamiento de los riesgos identificados.

3.2.4. Inventario de Activos

En la tabla 3-2, se muestra una lista de activos de información y el propietario correspondiente:

Tabla 3-2 Activos de información y propietarios funcionales

Nº	Activo de información	Propietario funcional
1	Programa SGA Claro	Jefe de Operaciones
2	Mini ERP-DSW	Jefe de Operaciones
3	Antivirus Sophos	Encargado de Sistemas
4	Microsoft Office 2013	Jefe de Operaciones
5	Escritorios	Personal de Operaciones
6	SCTR	Personal de Operaciones
7	EPP	Personal de Operaciones
8	Herramientas de trabajo	Personal de Operaciones
9	Equipo portátil (laptop)	Personal de Operaciones
10	PC de escritorio	Jefe de Operaciones

11	Antispam Sophos	Encargado de Sistemas
12	Correo corporativo	Encargado de Sistemas
13	Celular RPC	Personal de Operaciones
14	Informe de liquidación de gastos	Personal de Operaciones
15	Planilla de gastos de movilidad	Personal de Operaciones
16	Informe de TSS	Personal de Operaciones
17	Acta de visita	Personal de Operaciones
18	Informe de Radioenlace-microondas	Personal de Operaciones
19	Acta de instalación	Personal de Operaciones
20	Acta de servicio	Personal de Operaciones
21	Gráfica de topología de instalación	Personal de Operaciones
22	Fotos lado cliente y pop de instalación	Personal de Operaciones
23	Checklist del router	Personal de Operaciones
24	Guía de devolución	Personal de Operaciones
25	Guía de excedentes	Personal de Operaciones
26	Guía de remisión	Personal de Operaciones
27	Acta de mantenimiento correctivo	Personal de Operaciones
28	Acta de mantenimiento preventivo	Personal de Operaciones
29	Equipos backup	Personal de Operaciones
30	Windows Server	Jefe de Operaciones

31	Hoja de datos de trabajo	Jefe de Operaciones
32	SQL Server 2014	Encargado de Sistemas
33	Impresoras	Jefe de Operaciones
34	Reporte de Trabajo de mantenimiento correctivo	Jefe de Operaciones
35	Reporte de Programación de mantenimiento preventivo	Jefe de Operaciones
36	Reporte de programación de planta interna	Jefe de Operaciones
37	Reporte de programación de proyectos	Jefe de Operaciones
38	Reporte de Baja total de servicio	Jefe de Operaciones
39	Plan Anual de mantenimiento preventivo	Jefe de Operaciones
40	Métricas de trabajo de mantenimiento preventivo	Jefe de Operaciones
41	Backup de correo	Encargado de Sistemas
42	Backup de firewall	Encargado de Sistemas
43	Red Lan	Encargado de Sistemas
44	Teléfonos IP	Jefe de Operaciones
45	Internet	Encargado de Sistemas
46	VPN	Encargado de Sistemas
47	Red Wifi corporativo	Encargado de Sistemas
48	Equipos de medición	Personal de Operaciones
49	Windows 8	Personal de Operaciones

A continuación, en la tabla 3-3, se agruparán los activos de la información según sus características:

Tabla 3-3 Clasificación de activos de información

Nº	Grupos de activos de información	Activo de información
1	Software corporativo	Programa SGA Claro
		Mini ERP-DSW
2	Programas	Antivirus Sophos
		Microsoft Office 2013
		Antispam Sophos
		Windows Server
		SQL Server 2014
		Windows 8
3	Estaciones y equipos de trabajo	Equipo portátil (laptop)
		Escritorios
		PC de escritorio
		Impresoras
4	Equipos y herramientas de operaciones	SCTR
		EPP
		Herramientas de trabajo
		Celular RPC
		Equipos backup
		Equipos de medición
5	Servicios corporativos	Internet

		Correo corporativo
6	Datos almacenados	Informe de liquidación de gastos
		Planilla de gastos de movilidad
		Informe de TSS
		Acta de visita
		Informe de Radioenlace-microondas
		Acta de instalación
		Acta de servicio
		Gráfica de topología de instalación
		Fotos lado cliente y pop de instalación
		Checklist del router
		Guía de devolución
		Guía de excedentes
		Guía de remisión
		Acta de mantenimiento correctivo
		Acta de mantenimiento preventivo
		Hoja de datos de trabajo
		Reporte de Trabajo de mantenimiento correctivo
		Reporte de Programación de mantenimiento preventivo
		Reporte de programación de planta interna
		Reporte de programación de proyectos
		Reporte de Baja total de servicio
		Plan Anual de mantenimiento preventivo
		Métricas de trabajo de mantenimiento preventivo

7	Backup (copia de seguridad)	Backup de correo
		Backup de firewall
8	Redes de comunicaciones	Red Lan
		Teléfonos IP
		VPN
		Red Wifi corporativo

3.2.5. Valoración de los activos

En la tabla 3-4, se muestra la valoración de los activos de información, según sus atributos: confidencialidad, disponibilidad e integridad.

Tabla 3-4 Valoración de los activos de información

Nº	Activo de información	C	D	I	Total
1	Programa SGA Claro	MA	MA	A	MA
2	Mini ERP-DSW	MA	MA	A	MA
3	Antivirus Sophos	B	M	B	B
4	Microsoft Office 2013	B	M	B	B
5	Escritorios	B	B	B	B
6	SCTR	B	M	M	M
7	EPP	B	M	M	M
8	Herramientas de trabajo	M	M	M	M
9	Equipo portátil (laptop)	M	M	M	M

10	PC de escritorio	M	M	M	M
11	Antispam Sophos	B	M	B	B
12	Correo corporativo	A	A	M	A
13	Celular RPC	M	M	B	M
14	Informe de liquidación de gastos	M	M	M	M
15	Planilla de gastos de movilidad	M	M	M	M
16	Informe de TSS	M	A	A	A
17	Acta de visita	M	A	A	A
18	Informe de Radioenlace-microondas	M	A	A	A
19	Acta de instalación	M	A	A	A
20	Acta de servicio	M	A	A	A
21	Gráfica de topología de instalación	M	A	A	A
22	Fotos lado cliente y pop de instalación	M	A	A	A
23	Checklist del router	M	A	A	A
24	Guía de devolución	M	A	A	A
25	Guía de excedentes	M	A	A	A
26	Guía de remisión	M	A	A	A
27	Acta de mantenimiento correctivo	M	A	A	A
28	Acta de mantenimiento preventivo	M	A	A	A
29	Equipos backup	B	M	M	M

30	Windows Server 2012	B	M	M	M
31	Hoja de datos de trabajo	B	M	M	M
32	SQL Server 2014	B	M	B	B
33	Impresoras	B	B	B	B
34	Reporte de Trabajo de mantenimiento correctivo	M	A	A	A
35	Reporte de Programación de mantenimiento preventivo	M	A	A	A
36	Reporte de programación de planta interna	M	A	A	A
37	Reporte de programación de proyectos	M	A	A	A
38	Reporte de Baja total de servicio	M	A	A	A
39	Plan Anual de mantenimiento preventivo	M	A	A	A
40	Métricas de trabajo de mantenimiento preventivo	A	A	A	A
41	Backup de correo	M	M	M	M
42	Backup de firewall	M	M	M	M
43	Red Lan	A	A	A	A
44	Teléfonos IP	B	B	B	B
45	Internet	M	M	M	M
46	VPN	A	A	A	A
47	Red Wifi corporativo	A	A	A	A
48	Equipos de medición	M	M	M	M
49	Windows 8	B	M	M	M

3.2.6. Identificación de amenazas

En la tabla 3-5, se muestra la lista de amenazas por cada grupo de activos de información:

Tabla 3-5 Identificación de amenazas a los activos de información

Nº	Grupos de activos de información	Amenazas
1	Software corporativo	Acceso no permitido
		Falla de electricidad
		Falla de software
		Uso no autorizado de aplicación
		Abuso de los recursos de los sistemas
2	Programas	Mala instalación, configuración, actualización de software
		Instalación de software no licenciados
		Acceso al software por usuarios no autorizados
		Falta de soporte técnico apropiado para el software
		Infección por código malicioso, virus, troyanos, gusanos
3	Estaciones y equipos de trabajo	Error de usuario
		Falla de electricidad
		Deterioro de equipos
		Desinstalación de aplicativos y sistemas
		Robo de equipo
4	Equipos y herramientas de operaciones	Robo o pérdida de herramientas
		Mala manipulación de equipos
		Deterioro de herramientas

		Accidentes de trabajo
5	Servicios corporativos	Infección por código malicioso, virus, troyanos, gusanos, phishing
		Acceso al software por usuarios no autorizados
		Falta de soporte técnico apropiado para el software
		Perdida de información por caída de correos
		Falla de conexión del proveedor de servicio de internet
6	Documentación	Alteración de información
		Error de operador
		Fuga/Divulgación de información
		Robo o pérdida de documentos
		Información desactualizada – No disponible
7	Backup (copia de seguridad)	Falla en almacenamiento
		Error de operador
		Backup no autorizado
8	Redes de comunicaciones	Interrupción en los servicios
		Interceptación no autorizada de información en tránsito
		Entrega incorrecta de datos
		Falla de electricidad
		Error de operador

3.2.7. Posibilidad de ocurrencia de amenazas

En la tabla 3-6, se muestra la posibilidad de ocurrencia de las amenazas, según el grupo de activos correspondiente:

Tabla 3-6 Listado de amenazas y la posibilidad de su ocurrencia

Nº	Grupos de activos de información	Amenazas	Posibilidad de ocurrencia
1	Software corporativo	Acceso no permitido	A
		Falla de electricidad	A
		Falla de software	M
		Uso no autorizado de aplicación	M
		Abuso de los recursos de los sistemas	A
2	Programas	Mala instalación, configuración, actualización de software	A
		Instalación de software no licenciados	M
		Acceso al software por usuarios no autorizados	B
		Falta de soporte técnico apropiado para el software	M
		Infección por código malicioso, virus, troyanos, gusanos	M
3	Estaciones y equipos de trabajo	Error de usuario	M
		Falla de electricidad	M
		Deterioro de equipos	B
		Desinstalación de aplicativos y sistemas	M
		Robo de equipo	M
4	Equipos y herramientas de operaciones	Robo o pérdida de herramientas	M
		Mala manipulación de equipos	A
		Deterioro de herramientas	B
		Accidentes de trabajo	A

5	Servicios corporativos	Infección por código malicioso, virus, troyanos, phishing	M
		Acceso al software por usuarios no autorizados	B
		Falta de soporte técnico apropiado para el software	M
		Perdida de información por caída de correos	A
		Falla de conexión del proveedor de servicio de internet	M
6	Documentación	Alteración de información	A
		Error de operador	A
		Fuga/Divulgación de información	M
		Robo o pérdida de documentos	A
		Información desactualizada – No disponible	A
7	Backup (copia de seguridad)	Falla en almacenamiento	M
		Error de operador	M
		Backup no autorizado	B
8	Redes de comunicaciones	Interrupción en los servicios	B
		Interceptación no autorizada de información en tránsito	M
		Entrega incorrecta de datos	M
		Falla de electricidad	M
		Error de operador	B

3.2.8. Identificación de vulnerabilidades

En la tabla 3-7, se muestra una lista de vulnerabilidades, según los grupos de activos de información:

Tabla 3-7 Identificación de vulnerabilidades a los activos de información

Nº	Grupos de activos de información	Vulnerabilidades
1	Software corporativo	Errores en el software
		No se cuenta con sistema de respaldo de energía adecuado
		Falta de capacitación en los usuarios finales
		Configuración inadecuada
		Disponibilidad de herramientas que facilitan ataque
2	Programas	No existe con manuales de soporte para la solución de problemas.
		No se cuenta con un control para instalación de software
		No se cuenta con el control de accesos configurado por usuario
		Desconocimiento del personal de soporte para la
		No contar con antivirus o que esté desactualizado
3	Estaciones y equipos de trabajo	Error de usuario final
		No se cuenta con sistema de respaldo de energía adecuado
		Ausencia de programa de mantenimiento preventivo
		No se cuenta con un control para la desinstalación de aplicativos
		No existe un procedimientos estandarizado/Difundido para uso de equipos fuera / dentro de las instalaciones
4	Equipos y herramientas de operaciones	No existe un procedimientos estandarizado/Difundido para uso de equipos fuera / dentro de las instalaciones
		Ausencia de instructivos de soporte
		Ausencia de programa de mantenimiento preventivo
		Falta de seguro ocupacional y equipos de protección
5	Servicios corporativos	Ausencia de monitoreo del estado del antivirus

		No se cuenta con el control de accesos configurado por usuarios
		Desconocimiento del personal de soporte para la solución de problemas
		Falta de control de backup
		Tráfico de red
6	Documentación	Políticas de seguridad deficientes o inexistentes
		No se cuenta con Sistema de control de cambios/versiones.
		No existen políticas, cartas u otros documentos que evidencien confidencialidad de información.
		Falta de nivel de compromiso del colaborador con la empresa
		No contar un procedimiento para actualización de información
7	Backup (copia de seguridad)	Falla de dispositivo de almacenamiento
		Falla de aplicación de backup
		Backup no autorizado
8	Redes de comunicaciones	Políticas de seguridad deficientes o inexistentes
		Fallos en la autenticación
		Protocolos de red sin cifrar
		No se cuenta con sistema de respaldo de energía adecuado
		No existe segmentación de red ni filtros

3.2.9. Posibilidad de explotación de vulnerabilidades

En la tabla 3-8, se muestra la posibilidad de explotación de las vulnerabilidades, según los grupos de activos de información:

Tabla 3-8 Posible explotación de vulnerabilidades

Nº	Grupos de activos de información	Vulnerabilidades	Posibilidad de explotación
1	Software corporativo	Errores en el software	A
		No se cuenta con sistema de respaldo de energía adecuado	B
		Falta de capacitación en los usuarios finales	M
		Configuración inadecuada	M
		Disponibilidad de herramientas que facilitan ataque	A
2	Programas	No existen manuales de soporte para la solución de problemas.	M
		No se cuenta con un control para instalación de software	B
		No se cuenta con el control de accesos configurado por usuario	B
		Desconocimiento del personal de soporte para la solución de problemas	M
		No contar con antivirus o que esté desactualizado	M
3	Estaciones y equipos de trabajo	Error de usuario final	B
		No se cuenta con sistema de respaldo de energía adecuado	M
		Ausencia de programa de mantenimiento preventivo	B
		No se cuenta con un control para la desinstalación de aplicativos	B
		No existe un procedimientos estandarizado/Difundido para uso de equipos fuera / dentro de las instalaciones	M
4	Equipos y herramientas de operaciones	No existe procedimientos estandarizado/Difundido para uso de equipos fuera / dentro de las instalaciones	A
		Ausencia de instructivos de soporte	A
		Ausencia de programa de mantenimiento preventivo	M
		Falta de seguro ocupacional y equipos de protección	A

5	Servicios corporativos	Ausencia de monitoreo del estado del antivirus	B
		No se cuenta con el control de accesos configurado por usuarios	M
		Desconocimiento del personal de soporte para la solución de problemas	M
		Falta de control de backup	M
		Tráfico de red	B
6	Documentación	Políticas de seguridad deficientes o inexistentes	A
		No se cuenta con Sistema de control de cambios/versiones.	A
		No existen políticas, cartas u otros documentos que evidencien confidencialidad de información.	A
		Falta de nivel de compromiso del colaborador con la empresa	A
		No contar un procedimiento para actualización de información	A
7	Backup (copia de seguridad)	Falla de dispositivo de almacenamiento	M
		Falla de aplicación de backup	M
		Backup no autorizado	B
8	Redes de comunicaciones	Políticas de seguridad deficientes o inexistentes	M
		Fallos en la autenticación	M
		Protocolos de red sin cifrar	M
		No se cuenta con sistema de respaldo de energía adecuado	B
		No existe segmentación de red ni filtros	B

3.2.10. Estimado del Valor de los Activos en Riesgo

La siguiente tabla 3-9, muestra la evaluación del riesgo, a fin de determinar el daño cualitativo que el riesgo pudiera causar a los activos de información:

Tabla 3-9 Evaluación del riesgo

Nº	Grupos de activos de información	Amenazas	Posibilidad de ocurrencia	Posibilidad de Explotación	Valor de Activo de Información
1	Software corporativo	Acceso no permitido	A	A	AA
		Falla de electricidad	A	B	
		Falla de software	M	M	
		Uso no autorizado de aplicación	M	M	
		Abuso de los recursos de los sistemas	A	A	
2	Programas	Mala instalación, configuración, actualización de software	A	M	MM
		Instalación de software no licenciados	M	B	
		Acceso al software por usuarios no autorizados	B	B	
		Falta de soporte técnico apropiado para el software	M	M	
		Infección por código malicioso, virus, troyanos, gusanos	M	M	
3	Estaciones y equipos de trabajo	Error de usuario	M	B	MM
		Falla de electricidad	M	M	
		Deterioro de equipos	B	B	

		Desinstalación de aplicativos y sistemas	M	M	
		Robo de equipo	M	A	
4	Equipos y herramientas de operaciones	Robo de herramientas	M	A	AM
		Mala manipulación de equipos	A	M	
		Deterioro de herramientas	B	A	
		Accidentes de trabajo	A	B	
5	Servicios corporativos	Infección por código malicioso, virus, troyanos, phishing	M	M	MM
		Acceso al software por usuarios no autorizados	B	M	
		Falta de soporte técnico apropiado para el software	M	M	
		Perdida de información por caída de correos	A	B	
		Falla de conexión del proveedor de servicio de internet	M	B	
6	Documentación	Alteración de información	A	A	AA
		Error de operador	A	A	
		Fuga/Divulgación de información	M	A	
		Robo o pérdida de documentos	A	A	
		Información desactualizada – No disponible	A	A	
7	Backup (copia de seguridad)	Falla en almacenamiento	M	M	MM
		Falla de operador	M	M	

		Backup no autorizado	B	B	
8	Redes de comunicaciones	Interrupción en los servicios	B	M	MM
		Interceptación no autorizada de información en tránsito	M	M	
		Entrega incorrecta de datos	M	M	
		Falla de electricidad	M	B	
		Error de operador	B	B	

3.2.11. Posibilidad de Ocurrencia del Riesgo

En la tabla 3-10, se muestra la posibilidad de ocurrencia del riesgo según los activos de información.

Tabla 3-10 Listado de amenazas y la posibilidad de su ocurrencia

Nº	Grupos de activos de información	Amenazas	Vulnerabilidad	Valor de Activo de Información	Posibilidad de ocurrencia
1	Software corporativo	Acceso no permitido	Errores en el software	AA	A
		Falla de electricidad	No se cuenta con sistema de respaldo de energía		
		Falla de software	Falta de capacitación en los usuarios finales		
		Uso no autorizado de aplicación	Configuración inadecuada		

		Abuso de los recursos de los sistemas	Disponibilidad de herramientas que facilitan ataque		
2	Programas	Mala instalación, configuración, actualización de software	No existe con manuales de soporte para la solución de problemas.	MM	M
		Instalación de software no licenciados	No se cuenta con un control para instalación de software no licenciado		
		Acceso al software por usuarios no autorizados	No se cuenta con el control de accesos configurado por usuario		
		Falta de soporte técnico apropiado para el software	Desconocimiento del personal de soporte para la solución de problemas		
		Infección por código malicioso, virus, troyanos, gusanos	No contar con antivirus o que esté desactualizado		
3	Estaciones y equipos de trabajo	Error de usuario	Error de usuario final	MM	M
		Falla de electricidad	No se cuenta con sistema de respaldo de energía adecuado		
		Deterioro de equipos	Ausencia de programa de mantenimiento preventivo		
		Desinstalación de aplicativos y sistemas	No se cuenta con un control para la desinstalación de aplicativos		

		Robo de equipo	No existe un procedimientos estandarizado/ Difundido para uso de equipos fuera / dentro de las instalaciones		
4	Equipos y herramientas de operaciones	Robo o pérdida de herramientas	No existe un procedimientos estandarizado/ Difundido para uso de equipos fuera / dentro de las instalaciones	AM	A
		Mala manipulación de equipos	Ausencia de instructivos de soporte		
		Deterioro de herramientas	Ausencia de programa de mantenimiento preventivo		
		Accidentes de trabajo	Falta de seguro ocupacional y equipos de protección		
5	Servicios corporativos	Infección por código malicioso, virus, troyanos, phishing	Ausencia de monitoreo del estado del antivirus	MM	M
		Acceso al software por usuarios no autorizados	No se cuenta con el control de accesos configurado por usuarios		
		Falta de soporte técnico apropiado para el software	Desconocimiento del personal de soporte para la solución de problemas		
		Perdida de información por caída de correos	Falta de control de backup		
		Falla de conexión del proveedor de servicio de internet	Tráfico de red		
6	Documentación	Alteración de información	Políticas de seguridad deficientes o inexistentes	AA	A

		Error de operador	No se cuenta con Sistema de control de Cambios /versiones.		
		Fuga/Divulgación de información	No existen políticas, cartas u otros documentos que evidencien		
		Robo o pérdida de documentos	Falta de nivel de compromiso del colaborador con la empresa		
		Información desactualizada – No disponible	No contar un procedimiento para actualización de información		
7	Backup (copia de seguridad)	Falla en almacenamiento	Falla de dispositivo de almacenamiento	MM	M
		Error de operador	Falla de aplicación de backup		
		Backup no autorizado	Backup no autorizado		
8	Redes de comunicaciones	Interrupción en los servicios	Políticas de seguridad deficientes o inexistentes	MM	M
		Interceptación no autorizada de información en tránsito	Fallos en la autenticación		
		Entrega incorrecta de datos	Protocolos de red sin cifrar		
		Falla de electricidad	No se cuenta con sistema de respaldo de energía adecuado		
		Error de operador	No existe segmentación de red ni filtros		

3.2.12. Valor del Riesgo de los Activos.

En la tabla 3-11, se muestra la probabilidad de ocurrencia del riesgo y el impacto, según las amenazas identificadas.

Tabla 3-11 Valoración del riesgo

Nº	Amenazas	Probabilidad de ocurrencia	Impacto
1	Acceso no permitido	A	A
2	Falla de electricidad	M	M
3	Falla de software	M	M
4	Uso no autorizado de aplicación	A	A
5	Abuso de los recursos de los sistemas	M	M
6	Mala instalación, configuración, actualización de software	M	M
7	Instalación de software no licenciados	B	B
8	Acceso al software por usuarios no autorizados	A	A
9	Falta de soporte técnico apropiado para el software	M	M
10	Infección por código malicioso, virus, troyanos, gusanos, phishing	M	M
11	Error de usuario	M	M
12	Deterioro de equipos	B	B
13	Desinstalación de aplicativos y sistemas	M	M
14	Robo de equipo	B	B
15	Robo o pérdida de herramientas	M	M
16	Mala manipulación de equipos	A	M

17	Deterioro de herramientas	A	M
18	Accidentes de trabajo	M	M
19	Perdida de información por caída de correos	A	M
20	Falla de conexión del proveedor de servicio de internet	B	B
21	Alteración de información	A	M
22	Error de operador	A	M
23	Fuga/Divulgación de información	A	M
24	Robo o pérdida de documentos	A	M
25	Información desactualizada – No disponible	A	M
26	Falla en almacenamiento	A	M
27	Backup no autorizado	B	B
28	Interrupción en los servicios	A	M
29	Interceptación no autorizada de información en tránsito	A	M
30	Entrega incorrecta de datos	M	M

3.2.13. Mapa de calor

El mapa de calor permite representar de forma gráfica un plano conformado por la ubicación los riesgos de acuerdo a su probabilidad y su impacto.

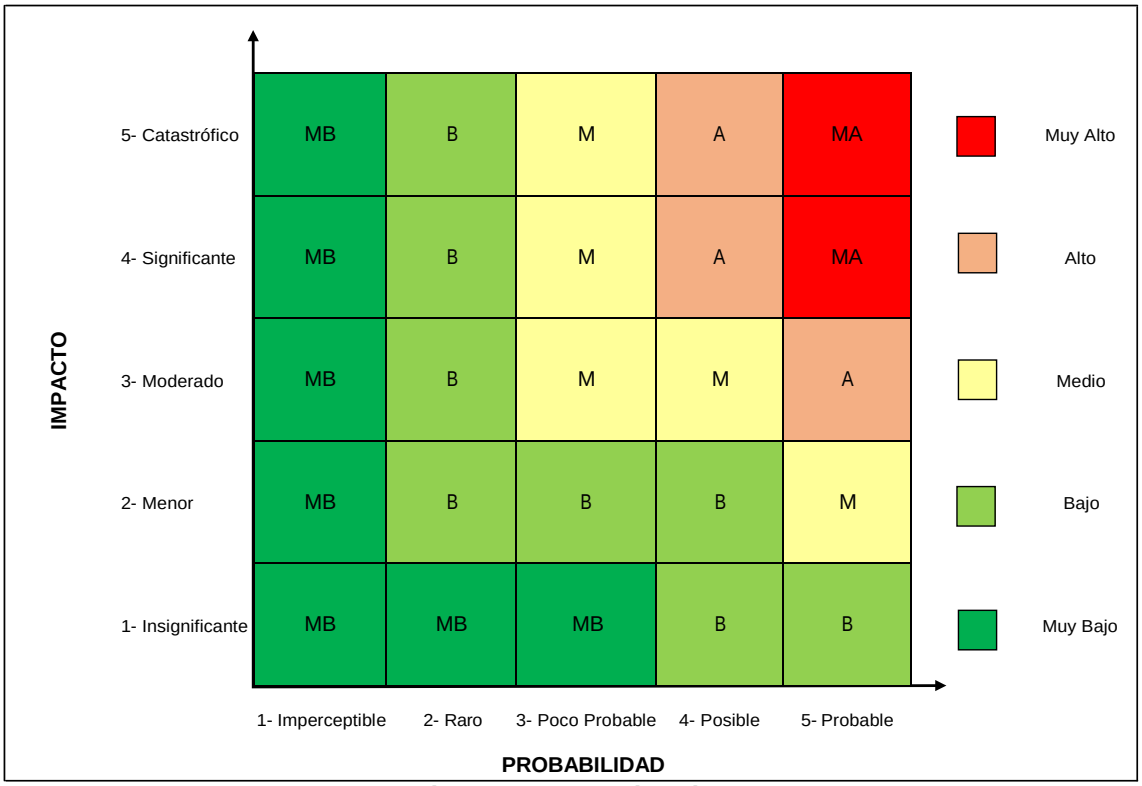


Figura 3-1 Mapa de calor
Fuente: Elaboración Propia

De acuerdo al mapa de calor, en la tabla 3-12 se identifica el nivel de los riesgos (probabilidad x impacto)

Tabla 3-12 Niveles del riesgo

Nº	Amenazas	Probabilidad de ocurrencia	Impacto	Nivel del riesgo
1	Acceso no permitido	A	A	Alto
2	Falla de electricidad	M	M	Medio
3	Falla de software	M	M	Medio
4	Uso no autorizado de aplicación	A	A	Alto
5	Abuso de los recursos de los sistemas	M	M	Medio
6	Mala instalación, configuración, actualización de software	M	M	Medio

7	Instalación de software no licenciados	B	B	Bajo
8	Acceso al software por usuarios no autorizados	A	A	Alto
9	Falta de soporte técnico apropiado para el software	M	M	Medio
10	Infección por código malicioso, virus, troyanos, gusanos, phishing	M	M	Medio
11	Error de usuario	M	M	Medio
12	Deterioro de equipos	B	B	Bajo
13	Desinstalación de aplicativos y sistemas	M	M	Medio
14	Robo de equipo	B	B	Bajo
15	Robo o pérdida de herramientas	M	M	Medio
16	Mala manipulación de equipos	A	M	Medio
17	Deterioro de herramientas	A	M	Medio
18	Accidentes de trabajo	M	M	Medio
19	Perdida de información por caída de correos	A	M	Medio
20	Falla de conexión del proveedor de servicio de internet	B	B	Bajo
21	Alteración de información	A	A	Alto
22	Error de operador	A	A	Alto
23	Fuga/Divulgación de información	A	M	Medio
24	Robo o pérdida de documentos	A	A	Alto
25	Información desactualizada – No disponible	A	M	Medio

26	Falla en almacenamiento	A	M	Medio
27	Backup no autorizado	B	B	Bajo
28	Interrupción en los servicios	A	M	Medio
29	Interceptación no autorizada de información en tránsito	A	M	Medio
30	Entrega incorrecta de datos	M	M	Medio

3.2.14. Tratamiento de riesgos

Se va a identificar y evaluar las distintas opciones de tratamiento de los riesgos. En la tabla 3-13, se muestra las opciones de tratamiento (mitigar, aceptar, evitar y transferir) para cada riesgo identificado.

Tabla 3-13 Opciones de tratamiento del riesgo

Nº	Amenazas	Probabilidad de ocurrencia	Impacto	Nivel del riesgo	Opción de tratamiento
1	Acceso no permitido	A	A	Alto	Mitigar
2	Falla de electricidad	M	M	Medio	Mitigar
3	Falla de software	M	M	Medio	Mitigar
4	Uso no autorizado de aplicación	A	A	Alto	Mitigar
5	Abuso de los recursos de los sistemas	M	M	Medio	Mitigar
6	Mala instalación, configuración, actualización de software	M	M	Medio	Mitigar
7	Instalación de software no licenciados	B	B	Bajo	Mitigar
8	Acceso al software por usuarios no autorizados	A	A	Alto	Mitigar

9	Falta de soporte técnico apropiado para el software	M	M	Medio	Mitigar
10	Infección por código malicioso, virus, troyanos, gusanos, phishing	M	M	Medio	Mitigar
11	Error de usuario	M	M	Medio	Mitigar
12	Deterioro de equipos	B	B	Bajo	Mitigar
13	Desinstalación de aplicativos y sistemas	M	M	Medio	Mitigar
14	Robo de equipo	B	B	Bajo	Mitigar
15	Robo o pérdida de herramientas	M	M	Medio	Mitigar
16	Mala manipulación de equipos	A	M	Medio	Mitigar
17	Deterioro de herramientas	A	M	Medio	Mitigar
18	Accidentes de trabajo	M	M	Medio	Transferir
19	Perdida de información por caída de correos	A	M	Medio	Mitigar
20	Falla de conexión del proveedor de servicio de internet	B	B	Bajo	Mitigar
21	Alteración de información	A	A	Alto	Mitigar
22	Error de operador	A	A	Alto	Mitigar
23	Fuga/Divulgación de información	A	M	Medio	Mitigar
24	Robo o pérdida de documentos	A	A	Alto	Mitigar
25	Información desactualizada – No disponible	A	M	Medio	Mitigar
26	Falla en almacenamiento	A	M	Medio	Mitigar
27	Backup no autorizado	B	B	Bajo	Mitigar

28	Interrupción en los servicios	A	M	Medio	Mitigar
29	Interceptación no autorizada de información en tránsito	A	M	Medio	Mitigar
30	Entrega incorrecta de datos	M	M	Medio	Mitigar

3.2.15. Selección de controles

De acuerdo a los requerimientos de seguridad, se han de identificar controles que garanticen que los riesgos sean reducidos a un nivel aceptable.

Los controles se consideran principios rectores para la administración de la seguridad de la información en la empresa. Para cada riesgo identificado existe una decisión de tratamiento de riesgo. En la tabla 3-14, se muestra los objetivos de control con sus respectivas salvaguardas para cada amenaza identificada.

Tabla 3-14 Selección de controles

Nº	Amenazas	Nivel del riesgo	Opción de tratamiento	Objetivos de control	Control	Tratamiento
1	Acceso no permitido	Alto	Mitigar	11.5 Control de acceso al sistema operativo.	11.5.1 Procedimientos seguros de inicio de sesión.	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
2	Falla de electricidad	Medio	Mitigar	9.2 Seguridad de los equipos.	9.2.2 Instalaciones de suministro.	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
3	Falla de software	Medio	Mitigar	8.2 Durante el empleo.	8.2.2 Concienciación, formación y capacitación en seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

4	Uso no autorizado de aplicación	Alto	Mitigar	11.2 Gestión de acceso de usuario.	11.2.2 Gestión de privilegios.	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
				11.6 Control de acceso a las aplicaciones y a la información.	11.6.1 Restricción del acceso a la información.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
5	Abuso de los recursos de los sistemas	Medio	Mitigar	11.5 Control de acceso al sistema operativo.	11.5.4 Uso de los recursos del sistema.	Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones.
6	Mala instalación, configuración, actualización de software	Medio	Mitigar	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Control de las vulnerabilidades técnicas.	Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas.

7	Instalación de software no licenciados	Bajo	Mitigar	15.1 Cumplimiento de los requisitos legales.	15.1.2 Derechos de propiedad intelectual (DPI).	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
8	Acceso al software por usuarios no autorizados	Alto	Mitigar	11.5 Control de acceso al sistema operativo.	11.5.2 Identificación y autenticación de usuario.	Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.
9	Falta de soporte técnico apropiado para el software	Medio	Mitigar	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Control de las vulnerabilidades técnicas.	Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas.

10	Infección por código malicioso, virus, troyanos, gusanos, phishing	Medio	Mitigar	10.4 Protección contra el código malicioso y descargable.	10.4.1 Controles contra el código malicioso.	Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.
				10.8 Intercambio de información.	10.8.4 Mensajería electrónica.	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
11	Error de usuario	Medio	Mitigar	8.2 Durante el empleo.	8.2.2 Concienciación, formación y capacitación en seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
12	Deterioro de equipos	Bajo	Mitigar	9.2 Seguridad de los equipos.	9.2.4 Mantenimiento de los equipos.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

13	Desinstalación de aplicativos y sistemas	Medio	Mitigar	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Control de las vulnerabilidades técnicas.	Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas.
14	Robo de equipo	Bajo	Mitigar	9.2 Seguridad de los equipos.	9.2.5 Seguridad de los equipos fuera de las instalaciones.	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
15	Robo o pérdida de herramientas	Medio	Mitigar	9.2 Seguridad de los equipos.	9.2.5 Seguridad de los equipos fuera de las instalaciones.	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

16	Mala manipulación de equipos	Medio	Mitigar	8.2 Durante el empleo.	8.2.2 Concienciación, formación y capacitación en seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
17	Deterioro de herramientas	Medio	Mitigar	9.2 Seguridad de los equipos.	9.2.4 Mantenimiento de los equipos.	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
18	Accidentes de trabajo	Medio	Transferir	No	No	Riesgo se transferirá a una compañía aseguradora La Positiva.
19	Perdida de información por caída de correos	Medio	Mitigar	10.5 Copias de seguridad.	10.5.1 Copias de seguridad de la información.	Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.

20	Falla de conexión del proveedor de servicio de internet	Bajo	Mitigar	10.2 Gestión de la provisión de servicios por terceros.	10.2.1 Provisión de servicios.	Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.
21	Alteración de información	Alto	Mitigar	10.7 Manipulación de los soportes.	10.7.3 Procedimientos de manipulación de la información.	Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados.
22	Error de operador	Alto	Mitigar	8.2 Durante el empleo.	8.2.2 Concienciación, formación y capacitación en seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

23	Fuga/Divulgación de información	Medio	Mitigar	10.7 Manipulación de los soportes.	10.7.3 Procedimientos de manipulación de la información.	Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados.
24	Robo o pérdida de documentos	Alto	Mitigar	10.7 Manipulación de los soportes.	10.7.4 Seguridad de la documentación del sistema.	Se debería proteger la documentación de los sistemas contra accesos no autorizados.
25	Información desactualizada – No disponible	Medio	Mitigar	8.2 Durante el empleo.	8.2.2 Concienciación, formación y capacitación en seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
26	Falla en almacenamiento	Medio	Mitigar	9.2 Seguridad de los equipos.	9.2.4 Mantenimiento de los equipos.	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

27	Backup no autorizado	Bajo	Mitigar	10.6 Gestión de la seguridad de las redes.	10.6.1 Controles de red.	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
28	Interrupción en los servicios	Medio	Mitigar	10.6 Gestión de la seguridad de las redes.	10.6.2 Seguridad de los servicios de red.	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
29	Interceptación no autorizada de información en tránsito	Medio	Mitigar	10.6 Gestión de la seguridad de las redes.	10.6.2 Seguridad de los servicios de red.	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
30	Entrega incorrecta de datos	Medio	Mitigar	10.6 Gestión de la seguridad de las redes.	10.6.1 Controles de red.	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

3.2.16. Políticas del PSI-DSW

Con el fin de optimizar el uso de la información, aplicaciones y sistemas de la empresa Desysweb, se dan las siguientes políticas de observancia general y obligatoria:

- Todo usuario con acceso a la información, aplicaciones o sistemas de la empresa tiene la obligación de adoptar todas las medidas de control establecidas, preservando su naturaleza confidencial y evitando su transferencia, modificación, destrucción o divulgación a entidades no autorizadas.
- Toda información que la infraestructura de sistemas, aplicaciones, programas transmiten o almacenan son propiedad de la empresa, por lo que ningún usuario puede copiar, duplicar, transmitir o divulgar dicha información. La información, propiedad de la empresa, está disponible únicamente para los usuarios que lo requieran dentro del estricto desempeño de sus funciones.
- Los nombres de usuario y contraseña secreta que son asignadas para el acceso a los sistemas, aplicaciones, y los recursos de la empresa, son personales, intransferibles y estrictamente confidenciales.
- Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para

establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

- La infraestructura de sistemas, aplicaciones y los recursos de la empresa deben ser utilizados únicamente para los fines laborales, no deberá ser usada para provecho personal, tales como entretenimientos, grupos de conversación, juegos recreativos, etc.
- La infraestructura de sistemas, aplicaciones y, los recursos de la empresa no deben ser usados para introducir o traficar con material obsceno, lujurioso o pornográfico, almacenar y/o solicitar mensajes o imágenes con orientación sexual, ni para provocar disgustos, ofensas y daño moral lo cual incluye hostigamiento a otros basado en raza, nacionalidad, sexo, orientación sexual, edad, religión, defecto físico o creencias políticas.
- Es responsabilidad de los jefes de área de la empresa, asegurarse que el personal a su cargo (contratado o no) conozca la presente normativa y cumpla con las disposiciones que requieren aprobación o supervisión previa al inicio de su trabajo
- La persona encargada de clasificar la información es la única que puede degradar su grado de confidencialidad.
- Está prohibido la instalación o ejecución de software no autorizado o sin licencia en cualquiera de los equipos de las áreas funcionales de la empresa.

- Los accesos de seguridad serán reevaluado o revocado de manera temporal o indefinidamente cuando un colaborador es promovido, hace uso de sus vacaciones, es despedido o transferido, esta política se aplica a toda la empresa que cuenten con acceso a los sistemas de información, equipos de cómputo o telecomunicaciones.
- Las copias de seguridad de la información y otros sistemas será almacenada con una antigüedad no mayor a un mes y se redundará en un servicio de almacenamiento en la nube o en un equipo que se encuentre en una ubicación diferente a del Data Center.
- Las copias de seguridad se realizaran diariamente de manera automática y a la media noche.
- Se mantendrá un chequeo constante del nivel de almacenamiento en los discos duros para evitar la saturación de los mismos.
- Se manejara un inventario de la realización de copias de seguridad de bases de datos detallando la fecha de backup, la hora, el tamaño, el responsable y las observaciones en el caso que existan.
- Los usuarios de las áreas funcionales de la empresa deberán contar con capacitaciones anualmente sobre la importancia de la seguridad de la información.
- Las claves de los servidores y equipos de telecomunicación deberán ser cambiadas cada seis meses o a la terminación o

cambio de empleo del personal que interactúa con estas claves.

- Todos los procedimientos de manipulación de los equipos de cómputo y telecomunicación relevantes deberán ser documentados, además deben incluir información del personal clave a ser contactado en caso de fallas no contempladas en los procedimientos de la documentación.
- Las claves usadas en los servidores y equipos de telecomunicación deberán contar con al menos 8 caracteres, incluirán números, letras mayúsculas y minúsculas, símbolos, y serán diferentes por cada equipo.
- Los equipos deben contar con sistemas de alimentación ininterrumpida para evitar la pérdida o daño de información durante un corte de energía eléctrica
- Implementar un plan de mantenimiento de servidores y equipos de telecomunicación de manera periódica, a fin de asegurar su operatividad y buen desempeño.
- La ubicación del data center o equipos de telecomunicación sensibles debe ser en lugares seguros de aniegos o inundaciones
- Se debe establecer un registro de control de entrada y salida a las áreas de la empresa.
- Cada vez que los usuarios de los ordenadores se alejen momentáneamente de sus respectivos equipos, deberá asegurarse de bloquear el equipo.

- Por ningún motivo, ninguna persona podrá retirar un equipo o componente de cómputo o telecomunicación de propiedad de la empresa, sin una guía de salía previamente autorizada por la dependencia en cuestión.
- Apagar los equipos cuando no se usaran por un largo periodo de tiempo.
- Los equipos deben estar inventariados, los riesgos de inventario deben mantenerse actualizados.
- La pérdida o robo de hardware debe ser reportada inmediatamente.
- Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en la empresa.
- Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida, tanto por entes internos o externos, para su posterior utilización en procesos legales de ser caso.
- Implementar un servicio de almacenamiento en la nube, para asegurar las copias de seguridad en caso de crisis o desastre.
- Los servidores deben contar con un sistema de redundancia en un ambiente externo de la ubicación actual del Data Center o en una nube, para asegurar la continuidad del negocio en caso de crisis o un desastre.

3.3. Revisión y consolidación de resultados

Los resultados obtenidos de este proyecto se derivan del desarrollo de las dos etapas que fueron establecidas para dar cumplimiento a los objetivos específicos que se establecieron con el propósito de poder alcanzar el objetivo general de proyecto.

Las etapas que se plantearon para llevar a cabo el proyecto son:

- Etapa 0-Para conocer el grado de conocimiento en seguridad de la información en la empresa Desysweb.
- Etapa 1- Planeamiento del PSI-DSW: Actividades que de acuerdo a la norma ISO 27001, se deben desarrollar para establecer el SGSI.

Los resultados de este proyecto se obtendrán de acuerdo a los objetivos específicos del proyecto:

3.3.1. Identificar y valorarlos activos de información.

Para la identificación de las áreas funcionales de la empresa Desysweb, se realizó cuestionarios a los socios de la empresa, para establecer la importancia de los activos de información en cada área. En la figura 3-2, se tiene en cuenta los servicios que ofrecen la empresa, los activos, la tecnología y procesos de las áreas funcionales; con una calificación de 0 a 5, según la importancia de las áreas funcionales.

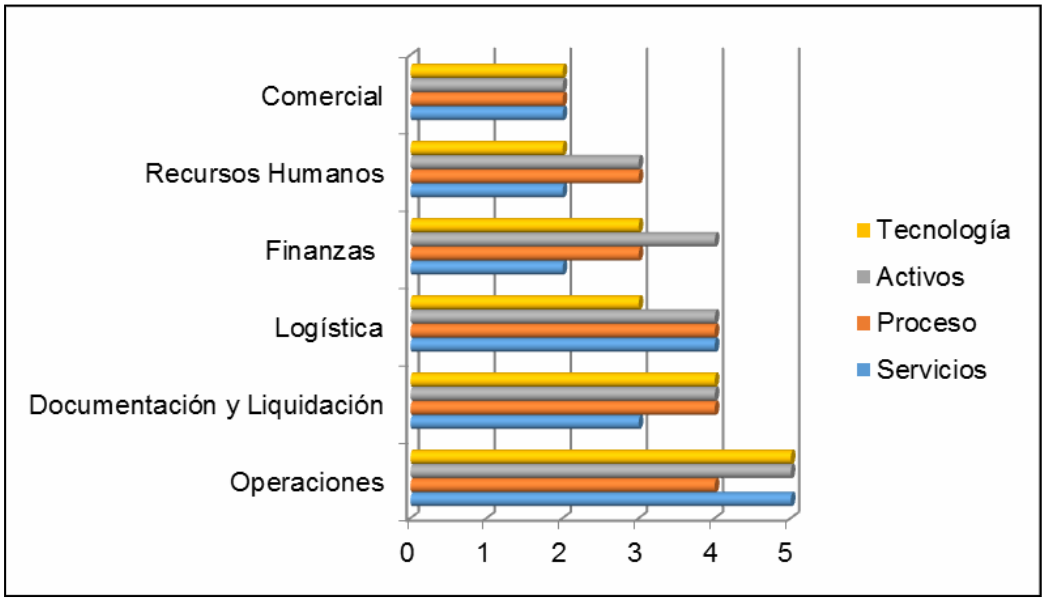


Figura 3-2 Importancia de las áreas funcionales
Fuente: Elaboración propia

En la figura 3-3, se muestra la valoración total de la gráfica anterior, obteniendo que el área funcional prioritaria es Operaciones y está incluida en el alcance del PSI-DSW.

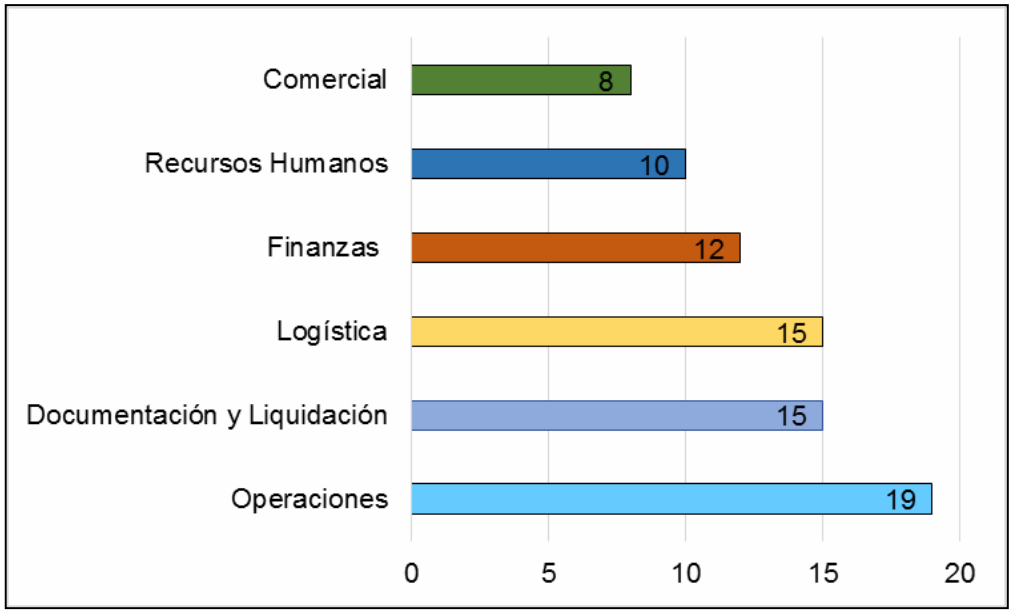


Figura 3-3 Valoración de las áreas funcionales prioritarias
Fuente: Elaboración propia

En caso de los activos de información, se tomó como referencia lo que los socios de la empresa nos mencionaron en los cuestionarios. Se identificó un total de 49 activos de información dónde en la tabla 3-15

Tabla 3-15: Número de activos identificados por grupo de activo

Grupos de activos de información	**Nº Activo**
Software corporativo	2
Programas	6
Estaciones y equipos de trabajo	4
Equipos y herramientas de operaciones	6
Servicios corporativos	2
Datos almacenados	23
Backup (copia de seguridad)	2
Redes de comunicaciones	4
Total	49

La Figura 3-4, indica la distribución de los activos de información por tipo de activo:

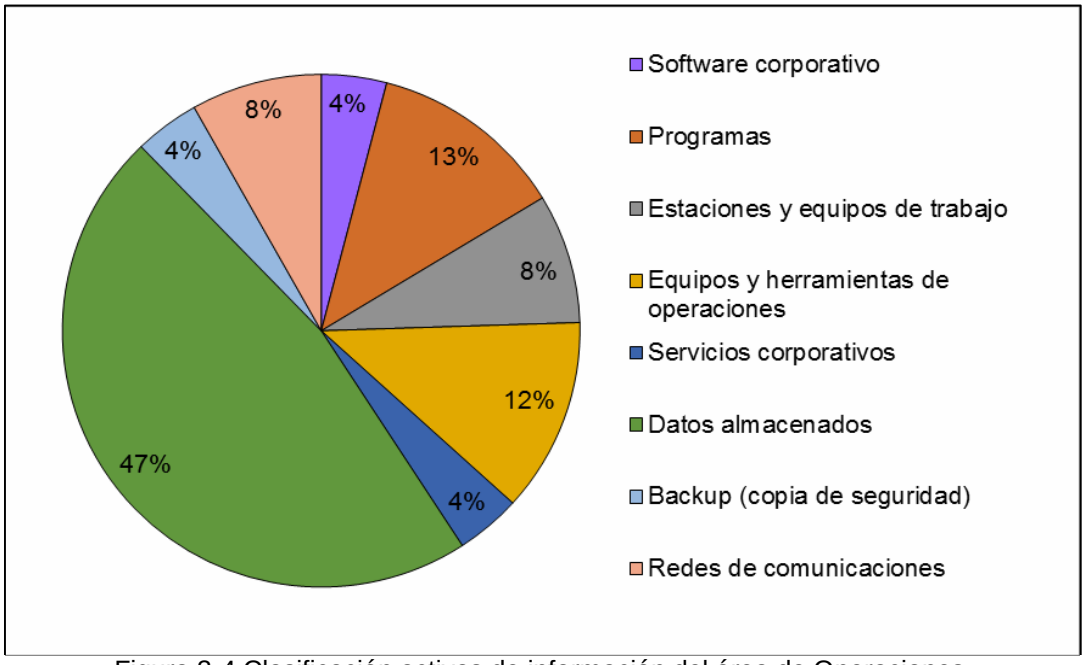


Figura 3-4 Clasificación activos de información del área de Operaciones
Fuente: Elaboración propia

- Los activos software corporativo representan el 4% de los activos de información, los cuáles incluye los sistemas que usa la empresa para realizar su operaciones.
- Los activos programas representan el 13% de los activos de información, están Microsoft Office, sistemas operativos, etc.
- Los activos de estaciones y quipos de trabajo representan el 8%, ahí se encuentran los escritorios, ordenadores, etc.
- El grupo de activos de Equipos y herramientas de operaciones representan el 12%, ahí incluye equipos de medición, herramientas de trabajo, etc.
- El grupo de activos de servicios corporativos representan el 4%, incluye correo corporativo e internet.
- Los activos datos almacenados representan el 47% de los activos de información, incluye la documentación respectiva del área.

- Los activos backup (copia de seguridad) representan el 4% de los activos de información, backup de correo y de firewall
- El grupo de activos de redes de comunicaciones representan el 8%, incluye red LAN, WIFI corporativos, etc.

3.3.2. Analizar y valorar los riesgos de seguridad de información asociados a los activos de información.

Una vez seleccionados los activos de información, se procedió a identificar las amenazas asociadas a éstos. La figura 3-5, muestra las amenazas identificadas y el número de los activos de información seleccionados que pueden ser afectados por éstas.

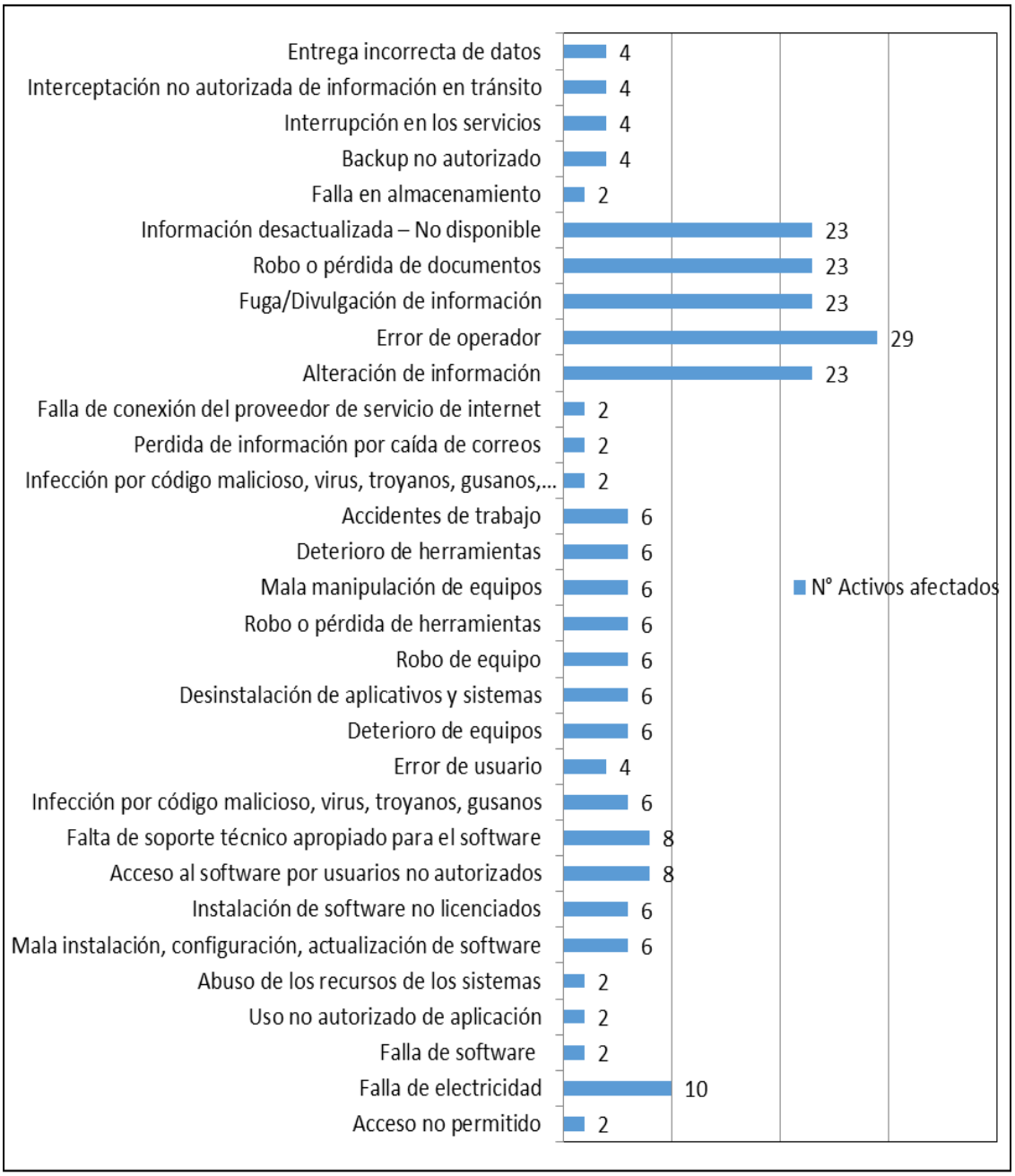


Figura 3-5 Cantidad de activos afectados por amenazas
Fuente: Elaboración propia

La grafica anterior muestra una visión de las amenazas internas o externas que pueden afectar la seguridad de la información de la organización. En la misma, se puede observar que la amenaza error del operador, puede poner en riesgos cada una de ellas, 29 de los 49 activos seleccionados, lo que equivale al 59% del total de estos activos. Así mismo, las amenazas

información desactualizada, robo o pérdida de documentos, fuga de información y alteración de información, puede afectar 23 activos que equivalen al 46% del total de los seleccionados.

Luego, en la figura 3-6, se identifica las posibles vulnerabilidades de los activos de información que pueden ser aprovechas por las amenazas identificadas.

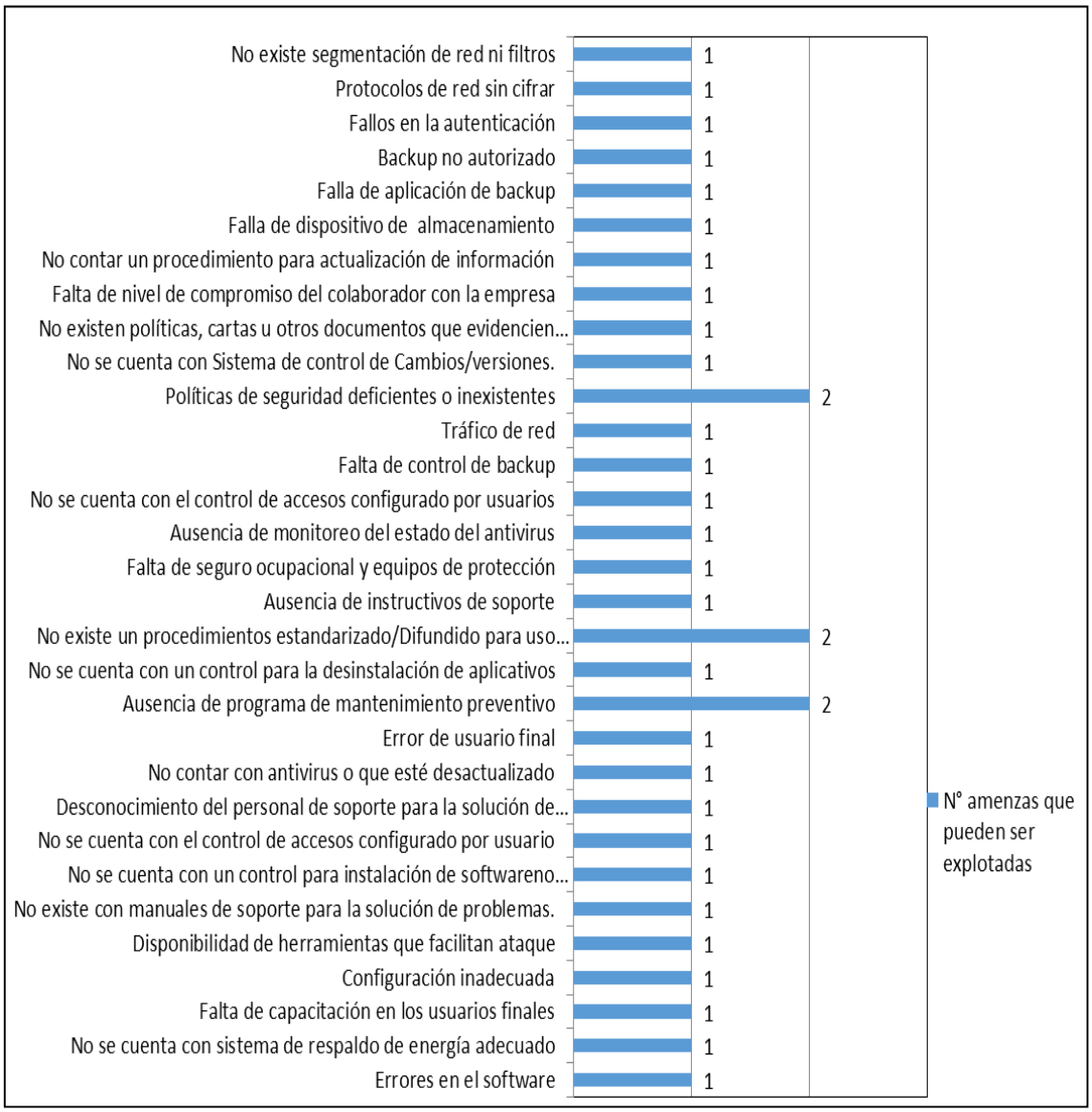


Figura 3-6 Vulnerabilidades y amenazas que pueden explotarlas
Fuente: Elaboración propia

Las vulnerabilidades que pueden ser aprovechadas por 2 de las amenazas identificadas, corresponde a la política de seguridad deficientes o inexistentes, no existe un procedimientos estandarizado para uso de equipos fuera o dentro de las instalaciones y ausencia de programas de mantenimiento preventivo., por lo tanto, es esencial que las políticas definidas del presente trabajo, sean aprobadas, publicadas e implementadas.

El resultado de valorar la probabilidad de ocurrencia y el impacto de las amenazas identificadas, se obtuvo el valor del riesgo de acuerdo a los datos y valores relacionados, ello se muestra en la figura 3-7.

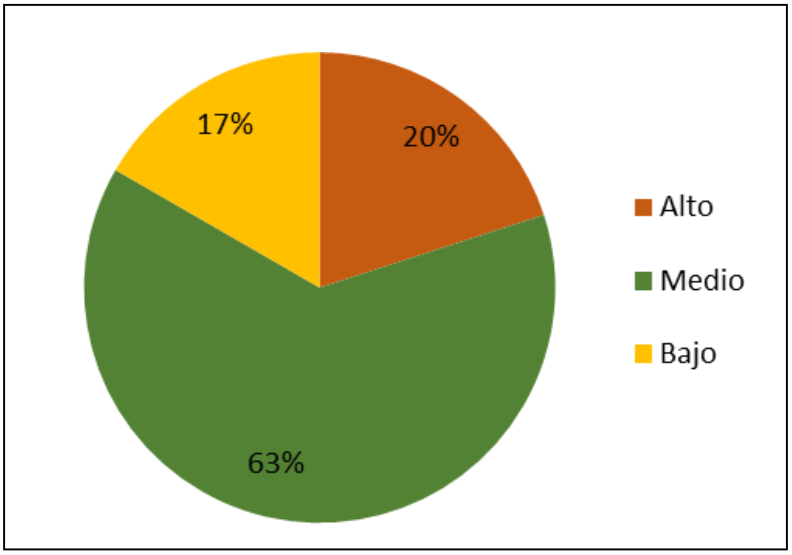


Figura 3-7 Niveles de riesgo
Fuente: Elaboración propia

De la gráfica se puede observar que, el 20% de los riesgos identificados tienen un nivel alto de riesgo, el 12% corresponde a los riesgos con un nivel bajo y el nivel medio de riesgos ocupa la mayor cantidad con un 63%.

3.3.3. Evaluar y recomendar los posibles controles adecuados para mitigar los riesgos.

Los controles o salvaguardas sirven para contrarrestar los efectos de los riesgos. Por ello, en la figura 3-8, se observan los controles y el número de riesgos que van a mitigar.

Figura 3-8 Controles y número de riesgos a mitigar
Fuente: Elaboración propia

En la gráfica se obtiene que cada control identificado va a mitigar al menos 1 riesgo. Siendo el control más utilizado el de concienciación, formación y capacitación en seguridad de la información, que va a mitigar a 5 riesgos.

Los controles van a ser utilizados para poder mitigar los riesgos y poder reducirlos a un nivel aceptable. El plan de tratamiento de riesgos se realiza en la siguiente fase de implementación.

3.4. Plan de Elaboración del Proyecto y Costos del Proyecto

3.4.1. Plan de Elaboración del Proyecto

La duración de este proyecto es de 3 meses, y las actividades se muestran en la tabla 3-16.

Tabla 3-16: Plan de Elaboración del Proyecto

N°	Actividades	Mes												Total de semanas
		Marzo				Abril				Mayo				
		1	2	3	4	1	2	3	4	1	2	3	4	
1	Identificación de activos													2
2	Valoración de activos													2
3	Identificación de amenazas													3
4	Identificación de vulnerabilidades													3
5	Análisis del riesgo													3
6	Tratamiento del riesgo													3
7	Propuesta de políticas de seguridad de información													3

3.4.2. Cronograma de Implementación del Proyecto

La duración de la implementación de los controles es de 5 meses, y las actividades se muestran en la tabla 3-17.

Tabla 3-17: Cronograma de Implementación del Proyecto

N°	Control	Meses / Semanas																				Total de semanas
		1				2				3				4				5				
1	Planeamiento de las otras áreas funcionales																					7
2	Seguridad ligada a los recursos humanos.																					10
3	Seguridad física y del entorno.																					10
4	Gestión de comunicaciones y operaciones.																					11
5	Control de acceso																					11
6	Adquisición, desarrollo y mantenimiento de sistemas de información.																					12
7	Cumplimiento																					12

3.4.3. Costos del Plan de Elaboración del Proyecto

Los costos del proyecto fueron asumidos por el proyectista en su totalidad. En la tabla 3-18, se muestran los costos:

Tabla 3-18: Costos del Plan de Elaboración del Proyecto

Recursos	Costos
Material de Impresión	120.00
Licencia de Office 2013	88.14
Equipo de Cómputo	375.00
Luz	90.00
Internet	269.70
Alimentos	720.00
Total	**S/. 1,662.84**

3.4.4. Costos de Implementación del Proyecto

A continuación se muestran los costos de implementación que incluyen costos de formación, recursos humanos y tecnología, se muestra en las tablas 3-19, 3-20, 3-21 y 3-22.

Tabla 3-19: Costos de Formación

Costos de Formación	Pago Total
Curso de Implementador Líder ISO 27001	2360.00
Total de Costos de Formación	**S/. 2,360.00**

Tabla 3-20: Costos de Recursos Humanos

Costos de Recursos Humanos	Pago mensual	Pago Total
Representante de la Alta Dirección de Desysweb SAC.	4500.00	22500.00
Coordinador del proyecton de seguridad de información	4000.00	20000.00
Ingeniero de seguridad de redes informáticas y de comunicación	3000.00	15000.00
Ingeniero de mantenimiento y reparación de equipos informáticos	3000.00	15000.00
Técnico profesional en computación e informática (redes informáticas y comunicación)	1500.00	7500.00
Asistente (con experiencia en ambientes informáticos)	1200.00	6000.00
Total en Recursos Humanos		**S/. 86,000.00**

Tabla 3-21: Costos de la Adquisición de Software

Costos de Adquisición de Software	Pago anual
Tracking and Recovery Service	142.37
Total de Costos de Adquisición de Software	**S/. 142.37**

Tabla 3-22: Costos de Tecnología

Costos de Tecnología	Pago mensual	Pago anual	Pago Total
Windows 8 (por volumen : 40 licencias)			719.06
Microsoft Office Standard 2013 (por volumen : 20 licencias)			1307.38
Windows Server 2012 R2			2883.00
SQL Server 2014 Standard			3043.00
Contanet (3 usuarios)	58.41	700.92	1777.79
Servidor HP			3399.00
Servidor cloud Amazon	2000	24898.82	24898.82
Antivirus Sophos		6153.36	6153.36
Firewall Sophos			19611.00
Zimbra Network Profesional Edition (ZCS): Profesional		6145.17	6145.17
Total de Costos de Tecnología	915.17		**S/. 69,937.58**

Total de Costos de Implementación	**S/. 158,439.95**

CONCLUSIONES

1. La determinación de las áreas funcionales ayudó a obtener el alcance del proyecto y su respectiva identificación de los activos de información en el área de Operaciones, vulnerabilidades y amenazas que requieren ser controladas para mitigar los riesgos.
2. Se logró desarrollar una buena metodología para la evaluación de los riesgos, así mismo identificar los riesgos que afecten a los activos de información y seleccionar los controles para disminuir el impacto de dichos riesgos en la empresa Desysweb.
3. También se llegó a la conclusión sobre la selección de los controles ayuda a poder salvaguardar los activos de la información y poder minimizar los riesgos, ello nos ayudará para el plan de tratamiento de riesgos que corresponde a la fase de implementación.
4. El activo más importante para la empresa Desysweb es la información, por tanto debe protegerse con mecanismos y controles que permitan mantener sus atributos de la seguridad de información: disponibilidad, integridad y confidencialidad.

RECOMENDACIONES

1. Se recomienda tener en la empresa un Sistema de Seguridad de la Información basado en la norma ISO 27001, además la implementación de la norma ISO 22301 que define los requisitos de los planes de continuidad del negocio, el análisis de impacto en el negocio, la estrategia de continuidad del negocio, etc.
2. Además, se recomienda promover la continuación de las fases restantes (implementación, monitoreo y revisión) del Sistema de Gestión de la Seguridad de la Información, con el fin de mejorar los procesos que se llevan actualmente en el área de Operaciones y en todas las áreas de la empresa, de igual manera se deben fomentar las buenas prácticas para proteger los activos de información.
3. Luego se deben realizar evaluaciones periódicas a las políticas de seguridad de la información y al sistema en general, esto con el fin de mantenerlas actualizadas y ajustadas a las necesidades del área de Operaciones y la empresa.
4. Finalmente, se recomienda que sea importante contar con el apoyo de la alta dirección, para que se conforme un equipo especializado y de esta manera se pueda implementar a futuro el sistema de gestión de seguridad de la información en el área de operaciones de la empresa Desysweb.

REFERENCIAS

Referencia Bibliográfica

1. Aguirre, R. y Zambrano, A. (2015). *Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001*. (Tesis de Grado, Universidad Nacional Abierta y a Distancia). Recuperado de http://repository.unad.edu.co/handle/10596/3655

2. Alexander, G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información*. Primera edición. Colombia: Ediciones Alfaomega.

3. Ampuero, C. (2011). *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros*. (Tesis de Grado, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

4. Barrantes, C. y Hugo, J. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos*. (Tesis de Grado, Universidad de San Martín de Porres). Recuperado de http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/609/3/barrantes_ce.pdf

5. Cabrales, A. (2016). *Gestión de Riesgos para la Dependencia Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña* (Tesis de Grado, Universidad Francisco de Paula Santander Ocaña).Recuperado de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/1074/1/28647.pdf

6. Castro, A. y Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Revista Científica Semestral de la Facultad de Ingeniería de la Universidad Distrital Francisco José de Caldas*, *16*(2). Recuperado de http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/3833/5399.
7. Chacón, P. (2012). *Propuesta de un modelo de sistema de gestión de seguridad de la información para institutos superiores tecnológicos de educación aeronáutica* (Tesis de Maestría, Escuela Politécnica Nacional de Ecuador). Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/7807/1/CD-4189.pdf
8. Cordero, K. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información* (Tesis de Grado, Universidad del Azuay). Recuperado dehttp://dspace.uazuay.edu.ec/bitstream/datos/5051/1/11490.pdf
9. Córdoba, A. (2015). *Diseño e implementación de un GGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001*. (Tesis de Grado, Universidad Nacional Abierta y a Distancia). Recuperado de http://repository.unad.edu.co/handle/10596/3627
10. Cortés, D. y Ardila, A. (2012). *Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 270001*. (Tesis de Grado, Universidad Privada EAN de Colombia). Recuperado de http://repository.ean.edu.co/handle/10882/2779

11. Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001: 2005 para una empresa de producción y comercialización de productos de consumo masivo*.(Tesis de Grado, Pontificia Universidad Católica del Perú). Recuperado dehttp://tesis.pucp.edu.pe/repositorio/handle/123456789/4957

12. Fernández, E.yPiattini, M. (2003). *Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada*. Primera edición. Madrid: Ediciones Aenor.

13. García, A. y Alegre, M. (2011). Seguridad informática. Primera Edición. Madrid: Ediciones Paraninfo SA.

14. Guzmán, A., yTaborda, C. (2015). Diseño de un sistema de gestión de la seguridad informática–SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá DC. (Tesis de grado, Universidad Nacional Abierta y a Distancia). Recuperado de http://hdl.handle.net/10596/3448

15. Guzmán, C. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso* (Tesis de Grado, Institución Universitaria Politécnico Gran Colombiano). Recuperado de http://alejandria.poligran.edu.co/handle/10823/746

16. Martelo, R., Madera, J. yBetín, A. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información tecnológica*, 26(2). Recuperado de http://dx.doi.org/10.4067/S0718-07642015000200015

17. Navarro, J., Díaz, M.y Marín, I. (2011). Planificación de políticas de seguridad. Escuela Superior Politécnica del Litoral de Ecuador. Recuperado de http://www.dspace.espol.edu.ec/handle/123456789/16199
18. Palacios, D. (2015). Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la norma ISO 27001: 2013. (Tesis de Grado, Universidad Nacional Abierta y a Distancia). Recuperado de http://66.165.175.249/handle/10596/3817
19. Pantaleone, F.y Silva, M. (2012). *Impacto de la ISO 27.000 en organizaciones: Estudio comparativo de herramientas para la implementación de un SGSI* (Tesis de Grado, Universidad Nacional de La Plata). Recuperado de http://hdl.handle.net/10915/47141
20. Sierra, O. (2011). *Estudio de los procesos de seguridad de la información digital en las empresas del departamento de Risaralda* (Tesis de Grado, Universidad Tecnológica de Pereira). Recuperado de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2370/0058S572.pdf?sequence=1&isAllowed=y
21. Valencia, N. (2013). Análisis, diseño e Implementación del sistema de gestión-Seguridad de la Informacion-SGSI en Emtelsa SAESP. (Tesis de Grado, Universidad de Manizales). Recuperado de http://ridum.umanizales.edu.co:8080/xmlui/handle/6789/153
22. Wu Fu, X. (2016). *Guía para la aplicación de las normas ISO 9001: 2015 e ISO 14001: 2015 a las empresas constructoras* (Tesis de

Grado, UniversidadPolitécnica de Catalunya). Recuperado de http://hdl.handle.net/2117/99518

Referencia Web

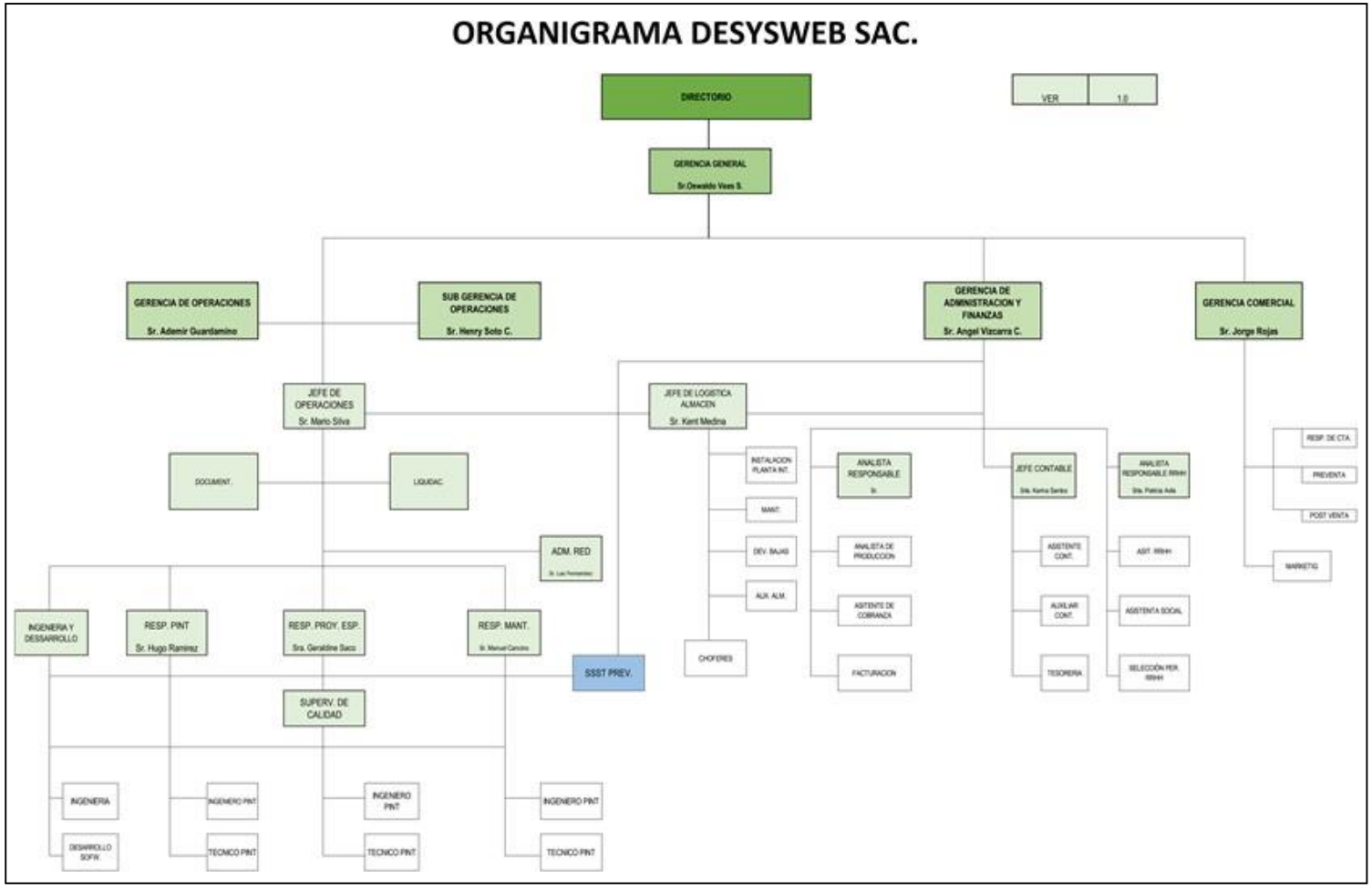
1. ISACA(s.f). *Redacción de COBIT 5.* Obtenido de http://www.isaca.org/COBIT/Pages/COBIT5Newsroom.aspx. Última fecha de consulta: 14 de Febrero de 2017.

2. ISO (s.f). *Concepto de SGSI.* Obtenido de http://www.iso27000.es/sgsi.html. Última fecha de consulta: 02 de Febrero de 2017.

3. SEI (s.f). *Evaluación del riesgo de seguridad de la información con el enfoque OCTAVE*. Obtenido de http://www.sei.cmu.edu/training /P10B.cfm**.**Última fecha de consulta: 18 de febrero de 2017.

ANEXOS

Anexo A



Anexo B

Cuestionario 1:

Nombre del Socio: Oswaldo Veas

- **¿Qué entiende por el concepto de seguridad de información?**

Es proteger la información a través de un software o sistema de información.

- **Los activos de información es aquello que genera o tiene valor para la empresa. Mencione algunos de los activos de información de la empresa Desysweb.**
  - Infraestructura
  - Equipos y herramientas
  - Sistema de información (SGA)
  - Estaciones de trabajo
  - Personal
  - Documentación
- **¿Cuáles son las políticas de seguridad de la empresa Desysweb?**
  - Se realiza el backup de correo y de firewall interdiario, y el servidor en la nube cada semana.
  - Los nombres de usuario y contraseña secreta que son asignadas para el acceso a los sistemas, aplicaciones, y los recursos de la empresa, son personales, intransferibles y estrictamente confidenciales.
  - La infraestructura de sistemas, aplicaciones y los recursos de la empresa deben ser utilizados únicamente para los fines laborales.

- La política de contraseñas es cambiarla mensualmente, especialmente la del correo corporativo y el cambio es mensual para evitar el phishing.
- Cada personal es responsable de los equipos y herramientas asignadas.

• **Los controles o salvaguardas son como el medio para manejar el riesgo. ¿Qué controles considera Ud. que se aplican en la empresa Desysweb?**

Aún no se tiene eso bien definido.

• **Considera Ud. que, ¿el personal de Desysweb tiene el grado de conocimiento sobre seguridad de información?**

Conscientemente no tienen mucho conocimiento en términos de seguridad de información, ello se demuestra en los incidentes que suceden en la empresa.

• **La ISO 27001 es una norma certificable en lo que corresponde a seguridad de información. ¿Qué opinión tiene sobre la propuesta del diseño de un sistema de gestión de seguridad de información para la empresa Desysweb, basado en la norma 27001?**

Se necesitaría la colaboración del personal y también los recursos económicos, pero si sería una propuesta interesante porque beneficiaría mucho a la organización.

• De las áreas funcionales que posee la empresa Desysweb, califique del 1 al 5 el nivel de importancia que tienen las siguientes categorías para cada área:

N	Área	Servicios	Proceso	Activos	Tecnología	Total
1	Operaciones	5	4	5	5	19
2	Documentación y Liquidación	3	4	4	4	15
3	Logística	4	4	4	3	15
4	Finanzas	2	3	4	3	12
5	Recursos Humanos	2	3	3	2	10
6	Comercial	2	2	2	2	8

Cuestionario 2:

Nombre del Socio: Henry Soto

- **¿Qué entiende por el concepto de seguridad de información?**

  Es proteger la información ante cualquier riesgo a través de un software.

- **Los activos de información es aquello que genera o tiene valor para la empresa. Mencione algunos de los activos de información de la empresa Desysweb.**

  - Infraestructura
  - Equipos y herramientas
  - Estaciones de trabajo
  - Personal
  - Documentación

- **¿Cuáles son las políticas de seguridad de la empresa Desysweb?**

  - Se realiza el backup de correo y de firewall interdiario, y el servidor en la nube cada semana.
  - Los nombres de usuario y contraseña secreta que son asignadas son personales, intransferibles y estrictamente confidenciales.
  - La infraestructura de sistemas, aplicaciones y los recursos de la empresa deben ser utilizados únicamente para los fines laborales.
  - La política de contraseñas es cambiarla mensualmente.
  - Cada personal es responsable de los equipos y herramientas asignadas.

- **Los controles o salvaguardas son como el medio para manejar el riesgo. ¿Qué controles considera Ud. que se aplican en la empresa Desysweb?**

Aún no se tiene eso bien definido.

- **Considera Ud. que, ¿el personal de Desysweb tiene el grado de conocimiento sobre seguridad de información?**

Conscientemente no se tiene una cultura de seguridad de información.

- **La ISO 27001 es una norma certificable en lo que corresponde a seguridad de información. ¿Qué opinión tiene sobre la propuesta del diseño de un sistema de gestión de seguridad de información para la empresa Desysweb, basado en la norma 27001?**

Se necesitaría la participación del personal y también los recursos económicos, pero si sería una propuesta interesante.

- De las áreas funcionales que posee la empresa Desysweb, califique del 1 al 5 el nivel de importancia que tienen las siguientes categorías para cada área:

N	Área	Servicios	Proceso	Activos	Tecnología	Total
1	Operaciones	4	4	5	4	17
2	Documentación y Liquidación	3	3	4	4	14
3	Logística	4	4	3	3	14
4	Finanzas	3	3	4	3	13
5	Recursos Humanos	2	4	3	2	11
6	Comercial	2	2	2	2	8

Cuestionario 3:

Nombre del Socio: Ademir Guardamino

- **¿Qué entiende por el concepto de seguridad de información?**

  Es proteger la información a través de políticas.

- **Los activos de información es aquello que genera o tiene valor para la empresa. Mencione algunos de los activos de información de la empresa Desysweb.**

  - Infraestructura
  - Equipos y herramientas
  - Sistema de información (SGA)
  - Estaciones de trabajo
  - Personal
  - Documentación
  - Servidores

- **¿Cuáles son las políticas de seguridad de la empresa Desysweb?**

  - Los nombres de usuario y contraseña secreta que son asignadas para el acceso a los sistemas, aplicaciones, y los recursos de la empresa, son personales, intransferibles y estrictamente confidenciales.
  - La infraestructura de sistemas, aplicaciones y los recursos de la empresa deben ser utilizados únicamente para los fines laborales.
  - Cada personal es responsable de los equipos y herramientas asignadas.

- **Los controles o salvaguardas son como el medio para manejar el riesgo. ¿Qué controles considera Ud. que se aplican en la empresa Desysweb?**

Aún no se tiene eso bien definido.

- **Considera Ud. que, ¿el personal de Desysweb tiene el grado de conocimiento sobre seguridad de información?**

Conscientemente no tienen mucho conocimiento en términos de seguridad de información, pero sería bueno concientizar al personal sobre ese concepto.

- **La ISO 27001 es una norma certificable en lo que corresponde a seguridad de información. ¿Qué opinión tiene sobre la propuesta del diseño de un sistema de gestión de seguridad de información para la empresa Desysweb, basado en la norma 27001?**

Se necesitaría mucha disposición del personal y también los recursos económicos, pero valdría la pena arriesgarse por aquello.

- De las áreas funcionales que posee la empresa Desysweb, califique del 1 al 5 el nivel de importancia que tienen las siguientes categorías para cada área:

N	Área	Servicios	Proceso	Activos	Tecnología	Total
1	Operaciones	5	4	5	5	19
2	Documentación y Liquidación	3	4	4	3	14
3	Logística	4	4	4	3	15
4	Finanzas	2	3	4	3	12
5	Recursos Humanos	2	3	3	2	10
6	Comercial	1	2	2	2	7

Cuestionario 4:

Administrador de Redes y Seguridad: Luis Fernández Patrocinio

- **¿Qué entiende por el concepto de seguridad de información?**

Es proteger la información a través de un software o sistema de información.

- **Los activos de información es aquello que genera o tiene valor para la empresa. Mencione algunos de los activos de información de la empresa Desysweb.**
  - Infraestructura
  - Equipos y herramientas
  - Sistema de información (SGA)
  - Estaciones de trabajo
  - Personal
  - Documentación
  - Servidores
  - Backup
  - Software y hardware
- **¿Cuáles son las políticas de seguridad de la empresa Desysweb?**
  - Se realiza el backup de correo y de firewall interdiario, y el servidor en la nube cada semana.
  - Los nombres de usuario y contraseña secreta que son asignadas para el acceso a los sistemas, aplicaciones, y los recursos de la empresa, son personales, intransferibles y estrictamente confidenciales.

- La infraestructura de sistemas, aplicaciones y los recursos de la empresa deben ser utilizados únicamente para los fines laborales.
- La política de contraseñas es cambiarla mensualmente, especialmente la del correo corporativo y el cambio es mensual para evitar el phishing.
- Cada personal es responsable de los equipos y herramientas asignadas.
- Toda información que la infraestructura de sistemas, aplicaciones, programas transmiten o almacenan son propiedad de la empresa, por lo que ningún usuario puede copiar, duplicar, transmitir o divulgar dicha información. La información, propiedad de la empresa, está disponible únicamente para los usuarios que lo requieran dentro del estricto desempeño de sus funciones.
-

• **Los controles o salvaguardas son como el medio para manejar el riesgo. ¿Qué controles considera Ud. que se aplican en la empresa Desysweb?**

Aún no se tiene eso bien definido.

• **Considera Ud. que, ¿el personal de Desysweb tiene el grado de conocimiento sobre seguridad de información?**

Conscientemente no tienen mucho conocimiento en términos de seguridad de información, ello se demuestra en los incidentes que suceden en la empresa.

• **La ISO 27001 es una norma certificable en lo que corresponde a seguridad de información. ¿Qué opinión tiene sobre la propuesta del diseño de un sistema de gestión de seguridad de información para la empresa Desysweb, basado en la norma 27001?**

Se necesitaría la colaboración del personal y también los recursos económicos, pero si sería una propuesta interesante porque beneficiaría mucho a la organización.

- De las áreas funcionales que posee la empresa Desysweb, califique del 1 al 5 el nivel de importancia que tienen las siguientes categorías para cada área:

N	Área	Servicios	Proceso	Activos	Tecnología	Total
1	Operaciones	4	4	5	5	18
2	Documentación y Liquidación	3	4	4	4	15
3	Logística	4	4	4	3	15
4	Finanzas	2	3	4	3	12
5	Recursos Humanos	2	3	3	2	10
6	Comercial	2	2	2	2	8

Anexo C

Compromiso de Desysweb SAC.
Clientes Corporativos

Nuestra compañía permite asegurar que las empresas deban operar con la confianza de tener su infraestructura de TI, telecomunicaciones y fibra óptica en óptimas condiciones aprovechando las tecnologías de información y convertirlas en una ventaja que aporte valor, funcionalidad y flexibilidad.

Misión:

Brindar servicios especializados en tecnologías de la información enfocados en lograr incrementar la competitividad y productividad del cliente.

Visión:

Ser el socio estratégico de confianza y de primer nivel que permita a las empresas su sostenido crecimiento del negocio.

Somos un grupo de profesionales especialistas en consultoría, diseño, gestión de proyectos e implementación de soluciones de tecnología de la información (TI), telecomunicaciones y fibra óptica, incluyendo proyectos a la medida y llave en mano, permitiendo que los recursos de TI sean aprovechados al máximo y estén alineados con los objetivos corporativos del negocio.

Nuestro compromiso está basado en la satisfacción y excelencia del servicio al cliente para lo cual aplicamos las mejores prácticas reconocidas en el mundo TI como ITIL y Project Management PMI. Permitir a los clientes contar con soluciones a base de marcas líderes en su rubro y contar con una propuesta de valor basada en costo y beneficio con la finalidad de cumplir sus expectativas de negocio. A continuación, se detallan nuestros servicios:

- Productos de Optimización, Compresión y Aceleración de tráfico de aplicaciones.
- Productos de Seguridad Informática.
- Productos Inalámbricos WiFi y Radio-Enlaces.
- Productos de Análisis de Redes y Fibra Óptica.

- Productos de Gestión de Procesos TI.

- Montaje Físico e Instalación del Equipos o sistemas.
- Configuraciones especiales y Reprogramación de equipos.
- Mantenimiento Preventivo y Correctivo.
- Diagnóstico y Pruebas Especializadas.
- Tendido, Instalación y Conectorización de Cableado estructurado y fibra óptica.
- Pruebas, Medición y Certificación de cableado de redes de telecomunicaciones y fibra óptica.
- Soporte Técnico 8x5 y 24x7 on-site y on-call
- Mantenimiento Preventivo y Correctivo.
- Reparación de Equipos / Actualizaciones.
- Modificaciones Técnicas y Upgrades.
- Trabajos Técnicos (Elaboración de cables, adaptadores, etc.).
- Monitoreo y Troubleshooting de redes TI, telecomunicaciones y fibra óptica.
- Optimización de redes.
- Outsourcing de servicios.

Nuestro cliente más importante es Claro Servicios Empresariales, y somos una de las principales contratistas que ellos tienen en el mercado. No obstante, vale aclarar que todas las áreas funcionales son indispensables para la empresa; pero el área que atienden los requerimientos de Claro, es el área de Operaciones que incluye a las sub áreas de Mantenimiento, Instalaciones y Proyectos; siendo ella el área más importante para la empresa porque es la que nos genera más productividad y ganancias a la empresa.

Finalmente, estimados colaboradores se les hace mención que deben ser partícipes en las actividades para poder generar más productividad a la empresa y también ser proactivos en los servicios que ofrecemos.

Atte.

Oswaldo Veas Santa Cruz
Gerente General de Desysweb SAC.

Anexo D

Mantenimiento Preventivo
Clientes Corporativos
Plan de Trabajo

1. Antecedentes

Claro dentro de sus estándares de atención, programa mantenimientos preventivos para los equipos (CPEs) en que dan Servicios Corporativos. Se elabora este documento para dar un alcance de los procedimientos a ejecutar de acuerdo a la Topología implementada para nuestro Cliente Corporativo.

2. Objetivo

Detallar las acciones a realizar durante el Mantenimiento Preventivo, así lograr prever futuras averías de los equipos instalados en las sedes del Cliente y garantizar un servicio de calidad.

3. Plan de Trabajo

El plan de trabajo presentado comprende tres etapas las cuales son detalladas a continuación:

i. Verificación previa del estado de los equipos:

El personal de Mantenimiento realizará lo siguiente:

- ✓ Se conectará una laptop a la consola del equipo identificando correctamente el equipo a apagar.
- ✓ Verificar los recursos de memoria Flash, memoria RAM, así como la versión del sistema operativo (IOS) que posee el Router.
- ✓ Verificar los eventos ocurridos en el Router desde su instalación/ encendido mediante comando, el resultado será almacenado en la laptop. Esta información nos permite registrar el comportamiento histórico del Router.
- ✓ Por contingencia se archivará la configuración del Router en la laptop y algunos comandos como apoyo para la verificación del servicio luego del Mantenimiento.
- ✓ Verificar el clock del router y corregir en caso sea necesario.
- ✓ Digitar el comando de grabación de configuración así evitar pérdidas de configuración al apagar el equipo.
- ✓ Toma de fotos panorámicas de ubicación de los equipo.
- ✓ Toma de fotos del estado actual del equipo.
- ✓ Toma de los datos de las condiciones ambientales antes del Mantenimiento Preventivo.

ii. Ejecución de los Trabajos

El personal de Mantenimiento procederá a realizar lo siguiente:

- ✓ Notificar al CNOC el inicio del trabajo.
- ✓ Identificación de todo el cableado conectado a los diversos puertos del Router.
- ✓ Apagar el equipo, retirarlo del ambiente de Telecomunicaciones.
- ✓ Realizar la limpieza interna (si el equipo lo permite) y externa del Router (llevarlo a un sitio en donde este equipo pueda ser sopleteado evitando ensuciar los demás equipos).
- ✓ Realizar limpieza externa del media converter y sus conectores, de los Jumpers de Fibra óptica y patch cord UTP.
- ✓ Realizar limpieza de bandeja y/o gabinete en donde se colocará el Router.
- ✓ Medición de los niveles de energía que alimentan los equipos.
- ✓ Colocar el equipo y conectorizar el cableado según las identificaciones antes colocadas.
- ✓ Conectar la laptop a la consola para registrar el encendido del equipo
- ✓ Energizarlo y reportar al CNOC el encendido del equipo.
- ✓ Verificar el servicio del cliente, realizando comandos que certifiquen conectividad.
- ✓ Confirmar la operatividad del circuito con el cliente.
- ✓ Cambio de etiquetas desgastadas (de equipos y/o cableado) en caso se requieran.
- ✓ Toma de fotos del equipo luego del Mantenimiento.
- ✓ Registro de todos los datos en el documento Acta de Mantenimiento Preventivo.

iii. Plan de Contingencia

El personal de Mantenimiento tiene como contingencia:

- ✓ Llevará los equipos de respaldo necesarios en caso de ocurrir alguna falla en el momento de realizar los trabajos.

4. Observaciones

El personal de Mantenimiento cuenta con un kit de Mantenimiento que contiene:

- Laptop, cable consola, pulsera antiestática
- Desarmadores, alicates, cintillos, velcro, cinta doble impacto
- Equipo back up
- Alcohol isopropílico, brochas, paños
- Multímetro
- Etiquetas
- Cámara fotográfica

Mantenimiento Preventivo - Clientes Corporativos
Plan de Trabajo (Servicio TELEFONIA)

1. Antecedentes

Claro dentro de sus estándares de atención, programa mantenimientos preventivos para los equipos (CPEs) que dan Servicios Corporativos. Se elabora este documento para dar un alcance de los procedimientos a ejecutar de acuerdo a la Topología implementada para nuestro Cliente Corporativo.

2. Objetivo

Detallar las acciones a realizar durante el Mantenimiento Preventivo, así lograr prever futuras averías de los equipos instalados en las sedes del Cliente y garantizar un servicio de calidad.

3. Plan de Trabajo

El plan de trabajo presentado para el servicio de Telefonía comprende tres etapas las cuales son detalladas a continuación:

i. Verificación previa del estado de los equipos:

El personal de Mantenimiento realizará lo siguiente:

- ✓ Verificar el ambiente donde se encuentra el equipo media converter.
- ✓ Toma de los datos de las condiciones ambientales antes del Mantenimiento Preventivo.

ii. Ejecución de los Trabajos

El personal de Mantenimiento procederá a realizar lo siguiente:

- ✓ Notificar al CNOC el inicio del trabajo.
- ✓ Identificación de todo el cableado conectado a los diversos puertos del MC.
- ✓ Apagar el equipo, retirarlo del ambiente de Telecomunicaciones.
- ✓ Realizar limpieza externa del media converter y sus conectores.
- ✓ Realizar limpieza de bandeja y/o gabinete en donde se colocará el MC.
- ✓ Medición de los niveles de energía que alimentan los equipos.
- ✓ Colocar el equipo y conectar el cableado según las identificaciones antes colocadas.
- ✓ Reportar al CNOC el encendido del equipo.
- ✓ Verificar el servicio del cliente, realizando comandos que certifiquen conectividad.
- ✓ Confirmar la operatividad del circuito con el cliente.
- ✓ Cambio de etiquetas desgastadas (de equipos y/o cableado) en caso se requieran.
- ✓ Toma de fotos del equipo luego del Mantenimiento.
- ✓ Registro de todos los datos en el documento Acta de Mantenimiento Preventivo.

iii. Plan de Contingencia

El personal de Mantenimiento llevará los equipos de respaldo necesarios en caso de ocurrir alguna falla en el momento de realizar los trabajos.

4. Observaciones

El personal de Mantenimiento cuenta con un kit de Mantenimiento que contiene:

- ✓ Laptop, cable consola, pulsera antiestática
- ✓ Desarmadores, alicates, cintillos, velcro, cinta doble impacto
- ✓ Alcohol isopropílico, brochas, paños
- ✓ Multímetro
- ✓ Etiquetas
- ✓ Cámara fotográfica

5. Tiempo Estimado

La ventana máxima de tiempo de corte del Local Telephone Services es de 20 min.

Procedimiento para la realización de Mantenimientos Preventivos

1º Coordinación con el cliente

a. Llamada hacia el coordinador por parte del cliente (esta persona debe tener la jerarquía suficiente para coordinar accesos a las sedes remotas del cliente y poder decidir ventanas de mantenimiento)
b. Darle a conocer la necesidad y las ventajas de este mantenimiento preventivo. De la misma manera informarle en que consistiría y solicitar una ventana de mantenimiento para dicho trabajo, adicionalmente solicitar nombres de contactos y números móviles de los mismos..
c. Confirmar vía mail la realización del mantenimiento, en dicho mail se debe especificar la fecha y hora (de preferencia en formato 24 horas), si el cliente lo requiere asignarle el nombre y DNI del ingeniero que realizara el trabajo. Dejar claro las consecuencias que conllevara este mantenimiento (corte de servicio o uso de equipos backup). Este mail debe ser copiado al supervisor de Telmex.

2º Preparación de datos antes del Mantenimiento Preventivo

a. Solicitar al Supervisor de Telmex la creación de una CCR y una OT para dicho mantenimiento preventivo.
b. Ingresar remotamente al equipo del cliente con la finalidad de conseguir la configuración mas reciente de su Router. Dicha configuración deberá ser enviada al Ingeniero encargado del Mantenimiento para la preparación respectiva del equipo Backup.
c. Se deberá tener en cuenta para la preparación del Router de backup la versión de IOS, tarjeteria, memorias, etc.
d. En caso no se disponga de los equipos necesarios para la realización del mantenimiento preventivo (Routers, media converters, fibra, etc.) se deberá solicitar dichos equipos al Supervisor de Telmex
e. Asegurarse de tener las actas respectivas así como las etiquetas para dejar identificados los equipos a los cuales se le realizara mantenimiento preventivo.
f. Asegurarse de tener los implementos necesarios para la realización de un exitoso mantenimiento preventivo, tales como, notebook, la versión de IOS, Kit de mantenimiento preventivo(1), Actas de Mantenimiento Preventivo y equipos de backup.

3º Procedimiento durante el mantenimiento preventivo.

a. Se informa al NOC la hora de llegada al cliente y la ejecución del numero de CCR.
b. Conectarse al router vía consola y verificar los servicios antes de empezar con el mantenimiento preventivo, de la misma forma verificar si el servicio del cliente presenta problemas como CRC's, Late Collisions, Drops, etc.
c. Informar al cliente y al NOC que se empezara con el mantenimiento preventivo (Se explicara al cliente que tiene que apagar los equipos). NO se empezara con el trabajo sin antes obtener la conformidad de ambas partes(2).
d. Se deja identificado el cableado que viene conectado al Router garantizando que al instalarlo nuevamente se conservara el mismo orden.
e. Se procede a apagar el Router, desconectado los cables Ethernet y demás.

f. Si el cliente lo requiere se procede a instalar el equipo de backup para que no pierda su servicio durante el preventivo.
g. Se realiza la limpieza interna y externa del Router. En dicha limpieza se contempla el destapado del equipo así como la desinstalación de cada tarjeta anexa que tenga dicho router (módulos de voz, datos, etc.). Para este proceso se utilizara solo Aire Comprimido, Brocha en buen estado, Alcohol Isopropilico y un paño blanco. Con estos equipos se garantiza que ninguno de los circuitos internos del router o sus tarjetas se corrompan.
h. Al terminar con el router se atiende el media converter desconectándolo, verificando el estado de sus conectores de fibra y cobre.
i. Luego se realiza la limpieza y verificación del estado del Patch Cord UTP y los jumper de fibra. En dicha verificación se enfatiza el estado conectores de ambos elementos.
j. Se verifica que los conectores de la caja Panduit no presenten problemas.
k. Durante los procesos g y h se procede a actualizar el inventario de equipos del cliente, plasmando dicha información en los recuadros asignados en el Acta de Mantenimiento Preventivo.
l. De ser necesario se realizara una limpieza del entorno donde se encuentran instalados lo equipos del cliente.
m. Se procede a la reconexión completa del circuito del cliente, procurando mejorar la instalación inicial, tal como posición de la fibra, posición del Patch Cord, correcta conectorizacion a energía, seguridad de los equipos.
n. Se le solicita la verificación de los servicios al cliente y vía consola se realizan diversas pruebas de conectividad y calidad de servicio.
o. Al terminar exitosamente las pruebas se reporta al NOC la terminación del Mantenimiento Preventivo.
p. Se llena el Acta de Mantenimiento Preventivo con los datos obtenidos del cliente y del ambiente donde se encuentran los equipos, es aquí donde se realiza las diversas recomendaciones, tal como, la reubicación de equipos, el reemplazo de alguno, la protección contra polvo, etc.
q. Se procede a la firma del Acta no sin antes informa al cliente de los trabajos realizados, el estado en que queda su servicio y realizar las recomendaciones necesarias para una mejor operatividad de su equipo.

4º Registro de datos en el Sistema SGA

a. Se recibe el acta firmada por el cliente luego del mantenimiento preventivo.
b. Se registra en el modulo de control de cambios sección mantenimiento preventivo los datos de numero de acta, trabajo realizado, estado del mismo, fecha de realización, duración. Así mismo se añade las observaciones encontradas y se actualiza el Inventario de Equipos del Cliente
c. Luego de terminado el registro de datos en la sección mantenimiento preventivo, se procede al cierre de la OT. Aquí se registra el estado del trabajo, la fecha de programación e inicio, se identifica las actividades (3) realizadas y se redacta un breve informe sobre las acciones realizadas durante el mantenimiento preventivo.

Observaciones:
(1) Kit de Mantenimiento Preventivo (sugerido por el suscrito)

- Aire Comprimido
- Alcohol Isopropilico
- Paño Blanco
- Brocha en buen estado
- Desarmadores (estrella y plano)
- Alicate (universal y punta)
- Llaves Allen
- Medidor de Temperatura y Humedad
- Plástico protector para cuando se trabaje en área del cliente, a fin de no ensuciar.
- Guantes
- Mangas de plástico para el ingeniero (a fin de no ensuciarse)

(2) En caso de que la ventana de mantenimiento se bastante rígida por parte del cliente y el operador del NOC no diera el visto bueno para el inicio de trabajos se escala directamente con la Supervisora de Mantenimiento Preventivo.

(3) Se registraran actividades según preciario.

PROCEDIMIENTO OPERATIVO MANTENIMIENTO CORRECTIVO PLANTA INTERNA MCPI-PO-01

1 OBJETIVO

Este procedimiento establece los pasos a seguir para la ejecución del Servicio de Mantenimiento Correctivo Planta Interna.

2 ALCANCE

El presente documento es de aplicación a todo el personal que participa en el proceso de de Mantenimiento Correctivo Planta Interna desde la llamada del Cliente requiriendo la atención de la avería hasta su atención, la generación del OT (Orden de Trabajo) y la entrega de las actas de servicio.

3 REFERENCIAS

Procedimiento Operativo de manipulación, almacenamiento, embalaje, conservación y entrega	Código: ALM-PO-01
Procedimiento Operativo de Solicitud de Movilidad y Caja Chica	Código: CAJ-PO-01
Relación básica de equipos para mantenimiento correctivo	Código: MCPI -MR-01
Instructivo de Llenado de Acta	Código: MCPI-IN-01
Stock Actual Equipos Correctivos-Preventivos	Código: ALM-MR-02

4 DEFINICIÓN

4.1 Avería: Servicio que no cumple con los requisitos establecidos por el cliente u organización.

4.2 POP: Lugar donde se concentran los circuitos asignados a cada cliente.

4.3 NODO: Lugar de donde convergen los circuitos de los POP's.

4.4 NOC: Siglas que definen Network Operation Center (Centro de Operaciones de Red). Es el grupo de personas que reportan las averías a la Mesa de Servicios de CSD, solicita personal para dichas atenciones y monitorea los trabajos de nuestro personal en campo de manera remota. Así mismo es quien da el visto bueno (VºBº) al termino de los trabajos.

4.5 Usuario de Servicio: Persona que hace uso del servicio que brinda nuestros clientes (la empresa operadora)

5 LINEAMIENTOS GENERALES

5.1 El Coordinador de Mesa de Servicio es el responsable de la Calidad de Servicio de mantenimiento correctivo Planta Interna llevando a cabo el seguimiento y monitoreo de la performance del servicio y el escalamiento al supervisor de campo o jefe inmediato en caso exista una peligro en incumplimiento de los requisitos del servicio.

5.2 En el momento de la recepción para la atención de una avería, el coordinador de mesa de servicio deberá solicitar como información preliminar sobre el tipo de problema presentado y tipo de servicio del cliente, Y procederá a verificar si se cuenta con el equipo según Stock Actual Equipos Correctivos-Preventivos alcanzado por almacén o verificándolo en el sistema SAP, E ingresará en su base de datos "Estadistica[mes _ año]" la siguiente información:

5.2.1 Nombre de Cliente

5.2.2 Sede del Cliente

5.2.3 Orden de Trabajo (OT) (En caso de los trabajos programados por correo)
5.2.4 Nombre del Ingeniero

5.3 La asignación del reporte de avería deberá efectuarse en un plazo máximo de 3 minutos, asignando la atención de la incidencia al ingeniero de turno según consta en el Rol de Personal, código: MCPI-CR-01. Y le transfiere los siguientes datos :

5.3.1 Nombre y sede del cliente
5.3.2 Nombre de contacto
5.3.3 Pop
5.3.4 Hora de llamada
5.3.5 Noc
5.3.6 Circuito (CID)
5.3.7 Equipos Backup.
5.3.8 Problema Presentado
De existir dudas técnicas por parte del ingeniero de campo, se comunicará directamente con el NOC. (Escalamiento)

5.4 El Ingeniero de campo es el responsable de atender las averías reportadas por el Coordinador de Mesa de Servicio considerando los siguientes plazos:
5.4.1 Plazo de desplazamiento: 1hr 30min. Desde la llamada del NOC.
5.4.2 Plazo de Solución de avería: 2 hr 20 min.
Asimismo, deberá coordinar la disponibilidad de las llaves en los lugares correspondientes (Boga, POP Chinchón o Arriola) para llevar a cabo el proceso de solución de la avería.

5.5 El ingeniero, una vez que es asignado para la avería, es responsable de la coordinación y retiro del almacén de los equipos necesarios para el trabajo a realizar.

5.6 Como inicio de los trabajos, el ingeniero de campo llamará al NOC para proceder con las pruebas respectivas. En caso de tratarse de trabajos en el POP, se coordinara previamente con el Centro de Control para la desactivación de las alarmas.

5.7 Los Ingenieros de campo deberán escalar al coordinador de mesa de servicio y al supervisor del cliente sobre las soluciones provisionales a fin de aprobar la aplicación de las mismas.

5.8 Luego de terminada la atención de la avería, el ingeniero de campo procederá al llenado del Acta de Mantenimiento Correctivo de acuerdo a los lineamientos del Instructivo "Llenado de Acta", Código: MCPI-IN-01.

5.9 El ingeniero de campo, procederá a verificar la conformidad del servicio a través de las pruebas de servicio con el NOC. Dicha conformidad se evidenciará con la firma del ingeniero de campo y del usuario del servicio en el Acta de Mantenimiento Correctivo y en el llenado de la encuesta, sobre el desempeño de nuestro personal, en la misma acta. (Este llenado de la encuesta es sugerido por el personal de campo al cliente, siendo opcional para el cliente el llenado)

5.10 En caso que el trabajo se realice en el POP/NODO, el personal de campo recibirá solo la conformidad del CNS inmediatamente se retirara del POP/NODO reportando obligatoriamente su salida al Centro de control telefónicamente, para la activación de las alarmas.

5.11 El ingeniero de campo deberá devolver los equipos y repuestos cambiados, bajo el Procedimiento Operativo de Manipulación, Almacenamiento Embalaje, conservación y entrega, código: ALM-PO-01

5.12 El Coordinador de Mesa de Servicio debe cerrar la OT del servicio dentro de las 48 horas luego de terminada la avería y 72 horas los fines de semana.

5.13 Los ingenieros de campo deberán escalar al supervisor de campo y al supervisor del cliente sobre las soluciones provisionales

5.14 Las actas son entregadas al cliente la primera semana del siguiente mes o cuando el cliente lo indica, entregándoles un cargo dando así la conformidad.

5.15 El coordinador para alguna actividad ó requerimiento con el área de compras y Almacén se efectuará mediante el SAP BUSINESS ONE.

6 DESCRIPCIÓN DEL PROCEDIMIENTO

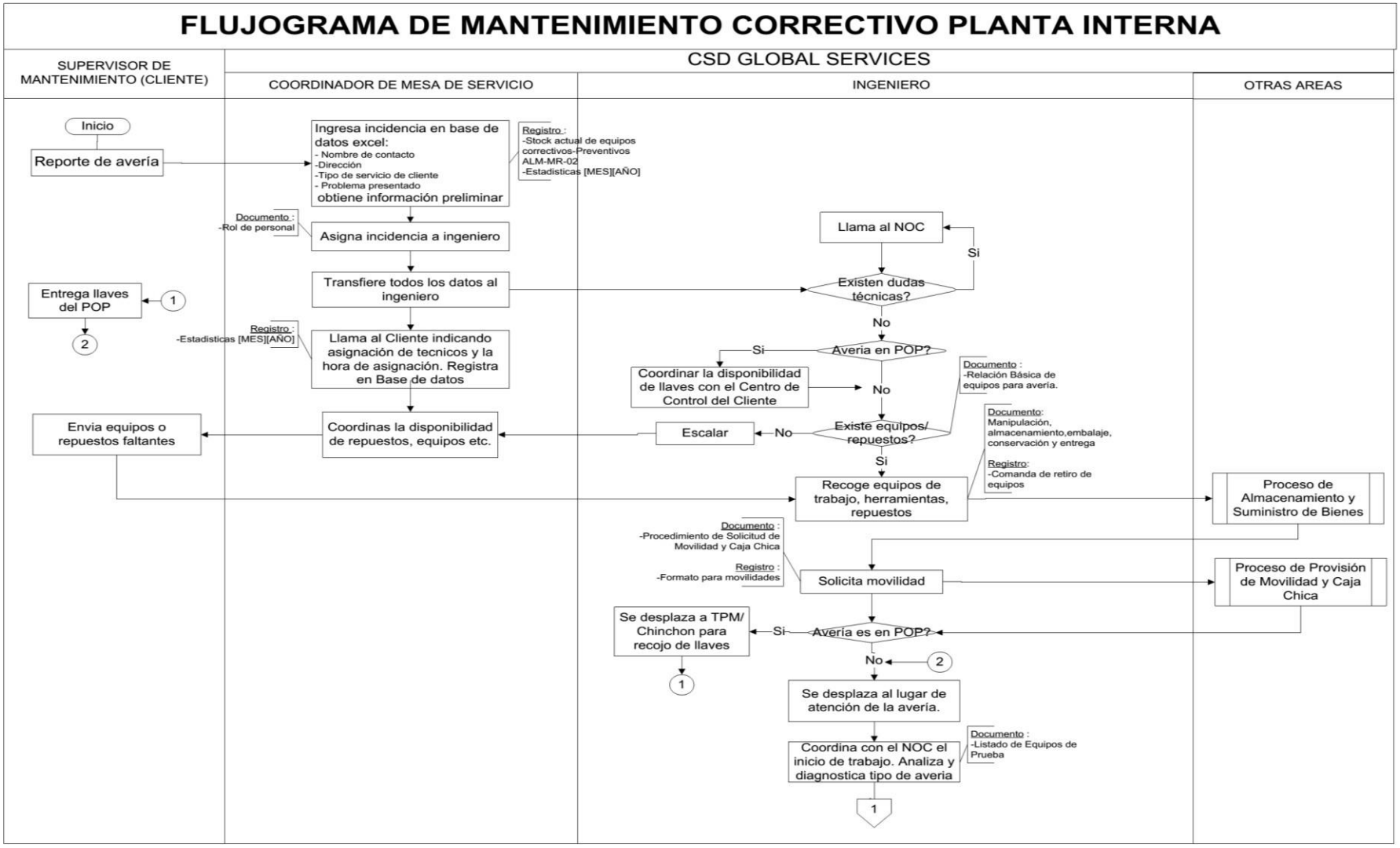
Ver anexo Nº 1

7 REGISTROS

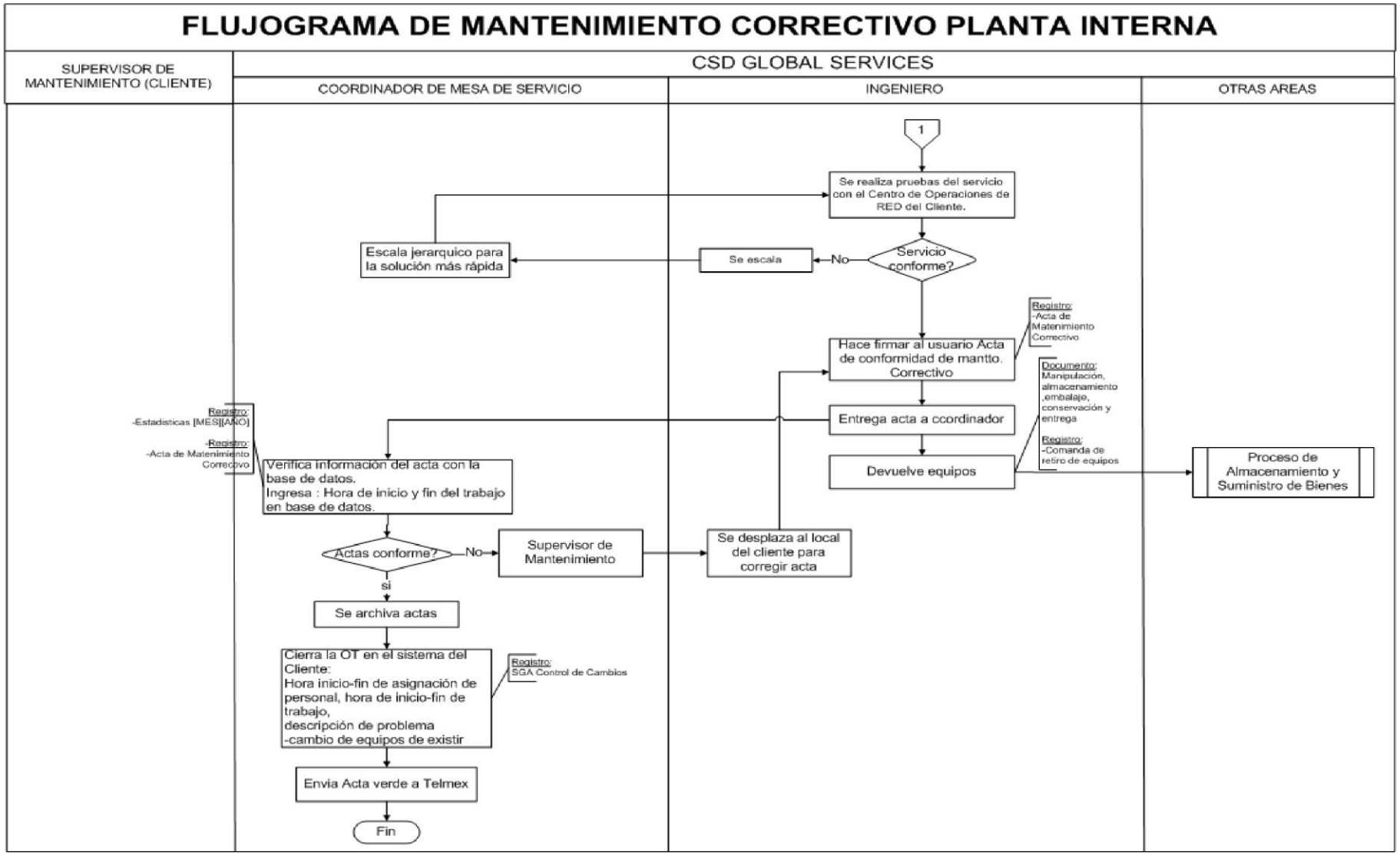
Estadísticas [mes][año]	Código: MCPI-PO-01-01
Acta de Mantenimiento Correctivo	Sin código
SGA: Control de Cambios	Sin código
Rol de personal	MCPI-CR-01

8 VIGENCIA DEL PROCEDIMIENTO

El presente procedimiento entra en vigencia el mismo día de su publicación.


FLUJOGRAMA DE MANTENIMIENTO CORRECTIVO PLANTA INTERNA
SUPERVISOR DE MANTENIMIENTO (CLIENTE)
CSD GLOBAL SERVICES
COORDINADOR DE MESA DE SERVICIO
INGENIERO
OTRAS AREAS
Inicio
Reporte de avería
Ingresa incidencia en base de datos excel:
- Nombre de contacto
-Dirección
-Tipo de servicio de cliente
- Problema presentado
obtiene información preliminar
Registro :
-Stock actual de equipos correctivos-Preventivos ALM-MR-02
-Estadisticas [MES][AÑO]
Documento :
-Rol de personal
Asigna incidencia a ingeniero
Transfiere todos los datos al ingeniero
Llama al NOC
Si
Existen dudas técnicas?
No
Averia en POP?
Si
Coordinar la disponibilidad de llaves con el Centro de Control del Cliente
No
Documento :
-Relación Básica de equipos para avería.
Entrega llaves del POP
1
2
Registro :
-Estadisticas [MES][AÑO]
Llama al Cliente indicando asignación de tecnicos y la hora de asignación. Registra en Base de datos
Envia equipos o repuestos faltantes
Coordinas la disponibilidad de repuestos, equipos etc.
Escalar
No
Existe equipos/ repuestos?
Si
Documento:
Manipulación, almacenamiento,embalaje, conservación y entrega
Registro:
-Comanda de retiro de equipos
Recoge equipos de trabajo, herramientas, repuestos
Proceso de Almacenamiento y Suministro de Bienes
Documento :
-Procedimiento de Solicitud de Movilidad y Caja Chica
Registro :
-Formato para movilidades
Solicita movilidad
Proceso de Provisión de Movilidad y Caja Chica
Se desplaza a TPM/ Chinchon para recojo de llaves
Si
Avería es en POP?
No
2
1
Se desplaza al lugar de atención de la avería.
Coordina con el NOC el inicio de trabajo. Analiza y diagnostica tipo de averia
Documento :
-Listado de Equipos de Prueba
1

FLUJOGRAMA DE MANTENIMIENTO CORRECTIVO PLANTA INTERNA



MANTENIMIENTO CORRECTIVO

HERRAMIENTAS BÁSICAS Y CABLEADO

1.-Desarmador estrella (107 rubicon).
2.-Desarmador plano (102 rubicon).
3.-Desarmador estrella pequeña (101 rubicon).
4.-Desarmador plano pequeño (101 rubicon).
5.-Alicate de Corte.
6.-Llave Ale Nº 4 y Nº 5
7. - Pulsera Antiestática.
8.- Cinta Making Tape ½".
9. - Cable directo Ethernet UTP.
10. - Cable cross Ethernet UTP.
11.- Cable consola.
12.- Cable Cross E1
13.- Cable serial DB9 directo.
14.- Loop de ethernet y E1.
15. -Conector DB25 a RJ45 (para Router 7200)

LO QUE DEBE TENER EL MALETIN DE CORRECTIVO ES:

1.- Laptop.
2.- Multitester.
3.-Crimping tool RJ45/RJ11.
4.-Conectores RJ45 /RJ11.

DOCUMENTACION Y EQUIPOS

1.-Acta Correctivo.
3.-Equipo Backup.
4.-Laptop.
5.-Fotocheck.

1.1 GENERAL

El presente documento comprende el desarrollo del nivel de ejecución en instalaciones, de las redes de datos y voz de los diversos servicios y productos de "Claro Perú" en las distintos locales de Clientes Corporativos y Estratégicos, a nivel Lima y Provincia.

1.2 ALCANCE DEL PROYECTO

El informe comprende la calidad y garantía de los servicios.

El trabajo realizado por DESYSWEB S.A.C., es un trabajo de buena calidad y mostrando la garantía del servicio.

1.2.1 Coordinación:

Elaboración previa de Información del Sistema de Claro (SGA) al mayor detalle, revisando y solicitando alcances de trabajos.

1.2.2 Ejecución

Personal preparado y capacitado para todos las metas y tareas, con todos los materiales y servicios requeridos para los proyecto.

1.2.3 Presentación

Entrega de servicios vía la documentación al día, y supervisión necesaria para un correcto y completo cierre de trabajos de acuerdo con las especificaciones de Claro Perú.

1.2.4 Temas

Requerimientos de Instalación de Última Milla Planta Interna (PINT) Pop + Cliente.

Procedimiento de Instalación de Última Milla Planta Interna (PINT) Pop + Cliente.

Etiquetado en el Pop con reflejo DDF de MC y DDF del equipo de acceso.

Secuencia de Fotos.

Configuraciones Básicas de Etiquetadora Brother.

Configuraciones Básicas de Etiquetadora Brother 2470.

REQUERIMIENTOS DE INSTALACIÓN DE ÚLTIMA MILLA PLANTA INTERNA (PINT) POP + CLIENTE.

A. INTRODUCCIÓN:

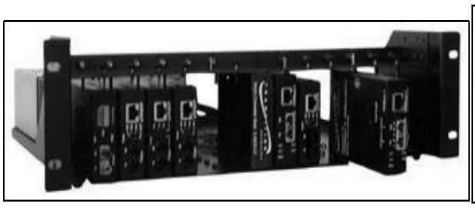
Instalación de Ultima Milla, es el nombre de la tecnología del nivel físico de la capa de transporte, con el cual mediante una tarjeta MC insertada en un chasis de alimentación electrónica realiza la conversión de señal de fibra óptica (luz laser – señales analógicas) a señal de cable UTP (señales digitales 1 y 0 en binario) para la codificación, segmentación de información o paquetes de datos y viceversa.

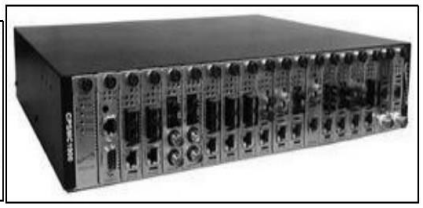
Consiste en realizar un enlace entre estos puertos ópticos mediante las terminaciones de Planta Externa (PEXT), ya sea enlace de Fibra Óptica Monomodo o Multimodo. Por lo tanto se necesita un lado local y remoto en este caso tenemos lado POP (Nodo de Interconexiones del Proveedor) y Lado Cliente (Equipos finales para el servicio).

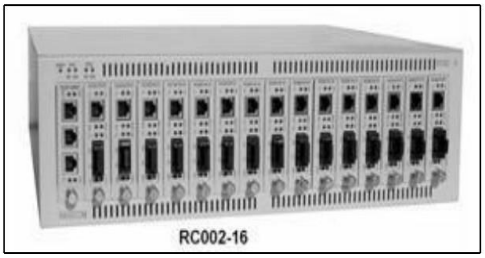
B. EQUIPAMIENTO LADO POP:

1. **Chasis de Media Converter (MC):** Son los equipos en cual se insertan las tarjetas MC, y ala vez son alimentadas por su fuente de alimentación, que son 2 Principal y Respaldo conectadas a diferentes tomas de Energía por obvias razones, este chasis MC tienen administración de gestión por un cable utp conectados a un Switch CLan, monitoreado por los equipos de la red del proveedor y por el operador CNS. Este setea la velocidad del enlace entre tarjetas MC, (Enlace de Ultima Milla).

   1.1 Marca y Modelos De Chasis MC: Transition Convertion Center 1600, Transition Point System 1800 y 1900, Raisecom de 16 Slots.



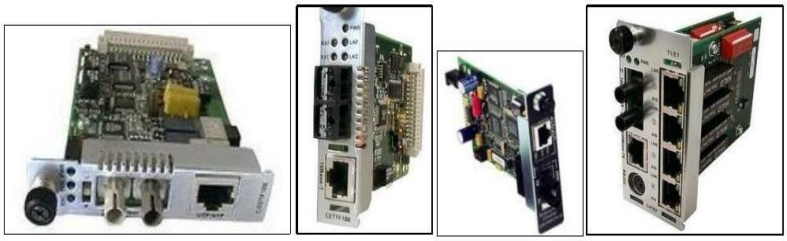




2. **Tarjeta de MC:** Son las de que cuentan con los puertos de conexión Óptica y Cu.

2.1 Marca y Modelos de Tarjetas MC: Son:

Transition para E1, Datos, Mux 4E1, MUX 4E1+1FE, etc.



Raisecom para E1, Datos, Mux 4E1, MUX 4E1+1FE, etc.

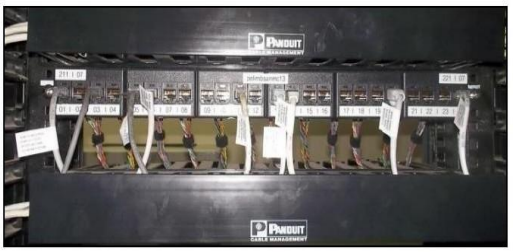
3. **Jumper de Fibra Óptica:** Son los siguientes

Jumper de Fibra Óptica Multimodo: Corto alcance de color Naranja, Fibra de 2 Hilos siempre del Modo Dúplex. Con los conectores ST-SC, SC-SC, ST-LC, SC-LC.

Jumper de Fibra Óptica Monomodo: Largo alcance de color Amarillo, Fibra de 2 y 1 Hilo. Con los conectores ST-SC, SC-SC, ST-LC, SC-LC, SC-FC

4. **Patch Cord UTP:** En el POP, solo usaremos de Categoría 5e, y también otras categorías dependiendo del requerimiento del servicio.

5. **Cableado Reflejo DDF:** Estos son los reflejos de cableado por medio de un cable multipar de 25 pares, conectados a un Patch Panel RJ45 desde el Chasis MC al Equipo de Acceso. Aquí se realiza la interconexión entre equipos si necesidad de tomar puertos directos.



Patch Panel Reflejo del MC.

Patch Panel Reflejo del E. Acceso.

6. **Terminaciones de Ópticas:** Parte Final de la instalación de ultima milla, en este dispositivo, se realiza las conexiones que emiten la señal de la tarjeta MC hacia el otro extremo del cliente mediante la calle, ductos, canalizado, subterráneos, postes, etc. De tal manera la empresa de PEXT liquida posición final para conexión. En Multimodo y Monomodo.

7. 

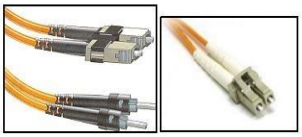
8. **Equipo de Acceso:** Equipo final del proveedor del servicio, ya sean Switch Cord, Router, (Red MPLS, ATM), Caja H (Red SDH), ONU, etc. Para los diferentes servicios requerido.

C. REQUERIMIETNOS LADO CLIENTE:

1. **Stand Alone:** Son los equipos del lado remoto, por el cual se recibe la señal del MC del POP mediante el enlace de Fibra Óptica, conectando los cables de Fibra, son Transition, Raisecom. En el caso de los equipos Raisecom se inserta una tarjeta MC.

2. **Jumper Fibra Óptica:**

   Jumper de Fibra Óptica Multimodo: Corto alcance de color Naranja, Fibra de 2 Hilos siempre del Modo Dúplex. Con los conectores ST-SC, SC-SC.



   Jumper de Fibra Óptica Monomodo: Largo alcance de color Amarillo, Fibra de 2 y 1 Hilo. Con los conectores ST-SC, SC-SC.

3. **Patch Cord:** En el Cliente, solo usaremos de Categoría 5e, y también otras categorías dependiendo del requerimiento del servicio.

4. **Router:** Es equipo principal para el servicio del cliente, configurado y revisado por el Ingeniero a cargo entregando el servicio con calidad y sin perdidas de paquetes. Servicios de Internet, RPV.

5. **Caja Panduit:** Es la terminación Optica, final que deja la empresa de PEXT, para realizar la conexión con el enlace directo al POP o NODO.

orios y Herramientas: Los accesorios constan de canaletas, conectores RJ45, Cinta Velcro, Doble Impacto, gado, etc., Herramientas Básicas.

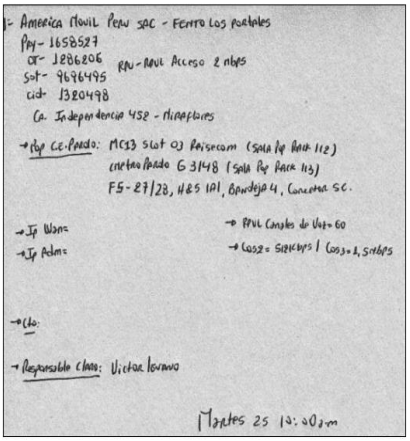
PROCEDIMIENTO DE INSTALACIÓN DE ÚLTIMA MILLA PLANTA INTERNA (PINT) POP + CLIENTE.

D. INTRODUCCIÓN:

Teniendo conocimiento de los requerimientos para la instalación de Ultima Milla, en el Pop + Cliente, se realiza el enlace con recursos de red y asignaciones de liquidación para las conexiones dando así la entrega del servicio solicitado por el cliente.

E. ASIGNACION DE TRABAJOS:

9. El coordinador de clientes asigna un documento de recursos. En el indica el Nombre de la razón social, dirección, tipo de servicio, recursos de red, asignación de MC, liquidación de PEXT, Puertos del equipo de acceso, Números PRY, OT, SOT y CID, nombre del contacto, etc. Los datos más importantes. El Personal de campo 01 Técnico, 01 Ingeniero.



10. El técnico tiene la responsabilidad de solicitar, verificar con mucho cuidado los equipos de la SOT asignada, leer el diseño de instalación para solicitar los materiales y accesorios.
11. Verificar la unidad móvil, solicitar al ingeniero apoyo para llevar las cosas.
12. Consultar por llaves del POP en seguridad de Claro, (Chinchón, Amov, Pueblo Libre, Aeropuerto, Villa, TPM). Asegurar que estén las llaves y reservarlos.
13. Salir de la oficina media o 1 hora antes al campo dependiendo del lugar, al campo.
14. Si tienes tiempo realizar Back to Back. O dejar al Ingeniero en cliente.

F. INSTALACION LADO POP:

1. Llamar al Centro de Control, indicando Nombre y empresa solicitando permiso para ingresar al POP.
2. Verificar si las asignaciones de recursos están disponibles, Chasis, PEXT, E. Acceso. (Problemas informar a Supervisor de Campo)
3. Insertar tarjeta en la asignación de UM.
4. Realizar el cableado de Fibra Óptica, con mucho cuidado.
5. Realizar el cableado de UTP, Patch Cord.
6. Conectar UTP al reflejo el Equipo de Acceso.
7. Informar al Ingeniero la verificación del Enlace FO, CU y asegurar las conexiones.
8. Etiquetar tomar fotos, informar salida al Centro de Control.

9. Presentación de Instalación.



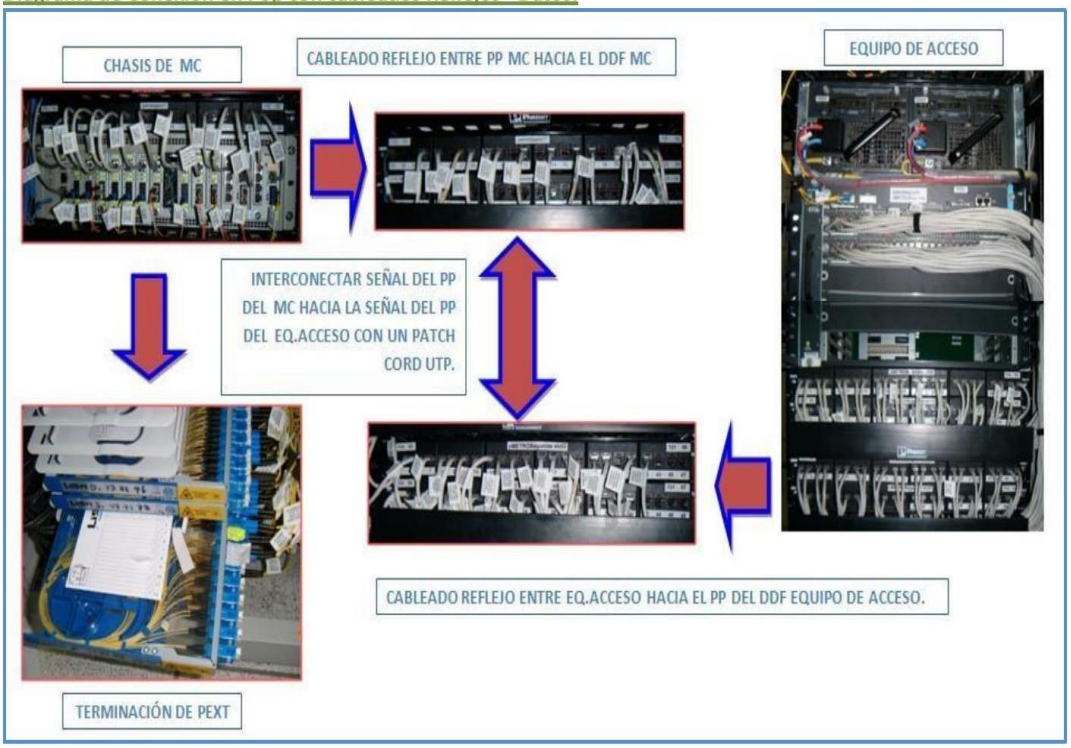
G. INSTALACION LADO CLIENTE:

1. Llegar 30 o 15 minutos antes al cliente. (Tec. Camisa o Chaleco – Ing. Saco y Corbata)
2. Identificarse (Fotocheck) saludar correctamente al contacto o cliente.
10. Verificar el diseño indicándole que se realizo un estudio previo. (Problemas informar a Supervisor de Campo)
3. Realizar la instalación con mucho cuidado, ya que en algunos sitios cuenta con tomas eléctricas delicadas, enlaces en producción, etc. (No cortes de servicio)
4. Si instalas gabinete, mucho cuidado con la conexión eléctrica del taladro, siempre conectarlo en una toma comercial.
5. Una vez enlazado, el Ingeniero es el encargado de llamar al CNS para empezar con la activación, indicándole los recursos de red, y dictando la Última Milla. (Si es E1 Pri lo realiza el Técnico).

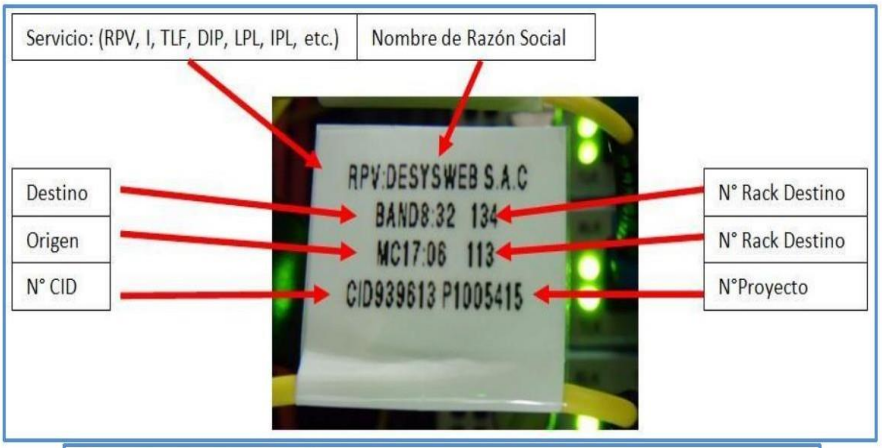
6. El ingeniero realiza la configuración del equipo Router y verificar informar la conectividad al técnico. Servicio Ok.
7. Ordenar la instalación, etiquetar, y tomar fotos.
8. Realizar actas de instalación, servicio, visita. Explicar lo básico con respecto al enlace y del servicio antes de realizar las firmas de actas el cliente.
9. Presentación de Instalación.

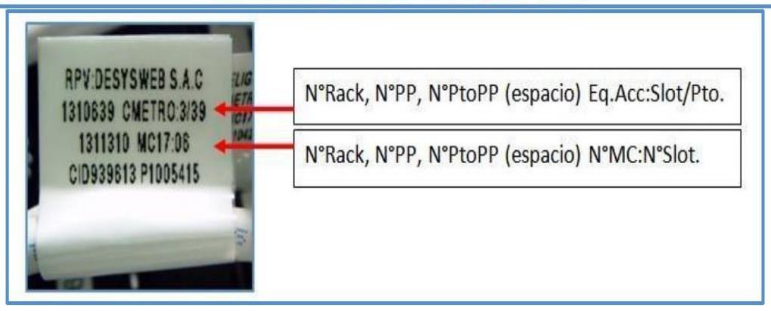
ETIQUETADO EN EL POP CON REFLEJO DDF DE MC Y DDF DEL EQUIPO DE ACCESO

Diagrama de Conexión en Pop con cableados Reflejos - Datos:



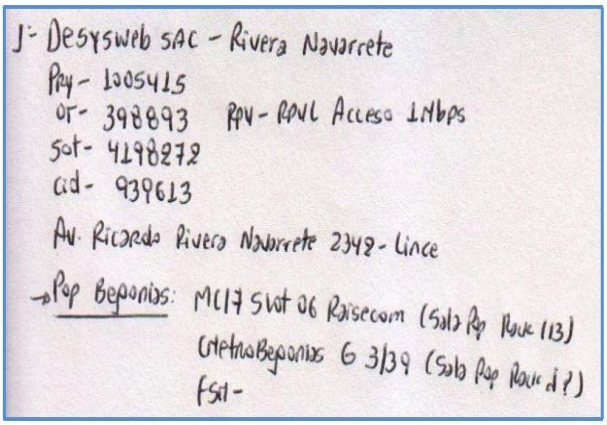
Detalle:





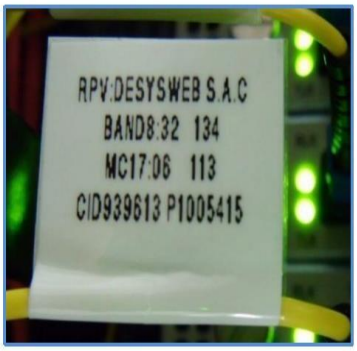
N°Rack: Número del Rack asignado.
N°PP : Número del Patch Panel.
N°PtoPP: Número del Puerto del Patch Panel.
Eq.Acc:Slot/Pto: Nombre de Equipo de Acceso: Slot de la Tarjeta / Puerto de la Tarjeta del Equipo de Acceso.
MC: Media Converter.
N°MC:N°Slot: Chasis de Media Converter : Slot asignado.

1. Se asigna los siguientes Recursos de Red:
   1.1 Ubicar el Chasis MC, identificar el número del Rack.
   1.2 Ubicar la terminación Óptica, identificar el número del Rack. (El Nº del Opticóm, Nº Panel GCO, Nº Bandeja H&S)
   1.3 Ubicar el Puerto reflejo del MC y Puerto reflejo del Equipo de Acceso.



Resumen Ejemplo:	
Bandeja 8: 32	Rack 134
MC17: 06	Rack 113
CmetroG3:/39	Rack 114

2. Empezamos por la etiqueta del Jumper de Fibra, en el MC y Terminación Óptica:

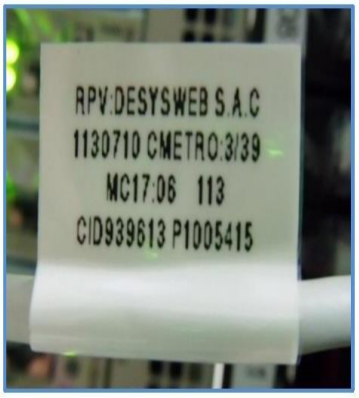


Etiqueta del Jumper lado MC
2da Línea - Destino - Posición PEXT. 3ra Línea – Origen - N°MC:N°Slot y N°Rack.

3. Etiquetamos en el lado de la terminación de Planta Externa (Opticom, GCO, Bandeja, etc):

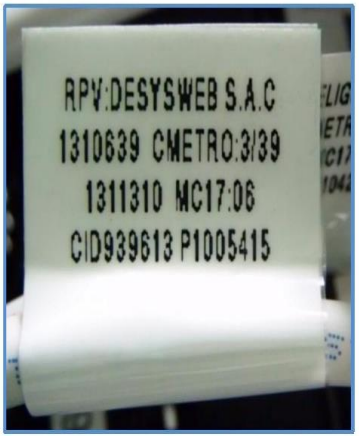
Etiqueta Jumper FO – Lado Terminación PEXT
2da Línea – Destino - N°MC:N°Slot y N°Rack. 3ra Línea - Origen - Posición PEXT.

4. Etiqueta del Patch Cord de 0.15 m. (Primer Patch Panel de UM):



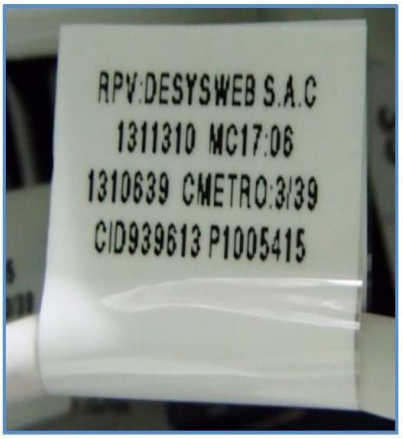
Etiqueta del Patch Cord del MC (al centro).
2da Línea – Destino: N°Rack, N°PP ,N°PtoPP y y Eq.Acc:Slot/Pto 3ra Línea – Origen: Posición N°MC:N°Slot y N°Rack.

5. Etiqueta del Cable que une El Reflejo del MC (DDF UM) con Reflejo Cmetro (DDF Equipo de Acceso):



Etiqueta del PP del Reflejo del MC
2da Línea – Destino: N°Rack, N°PP ,N°PtoPP y Eq.Acc:Slot/Pto. 3ra Línea – Origen: N°Rack, N°PP ,N°PtoPP y N°MC:N°Slot.

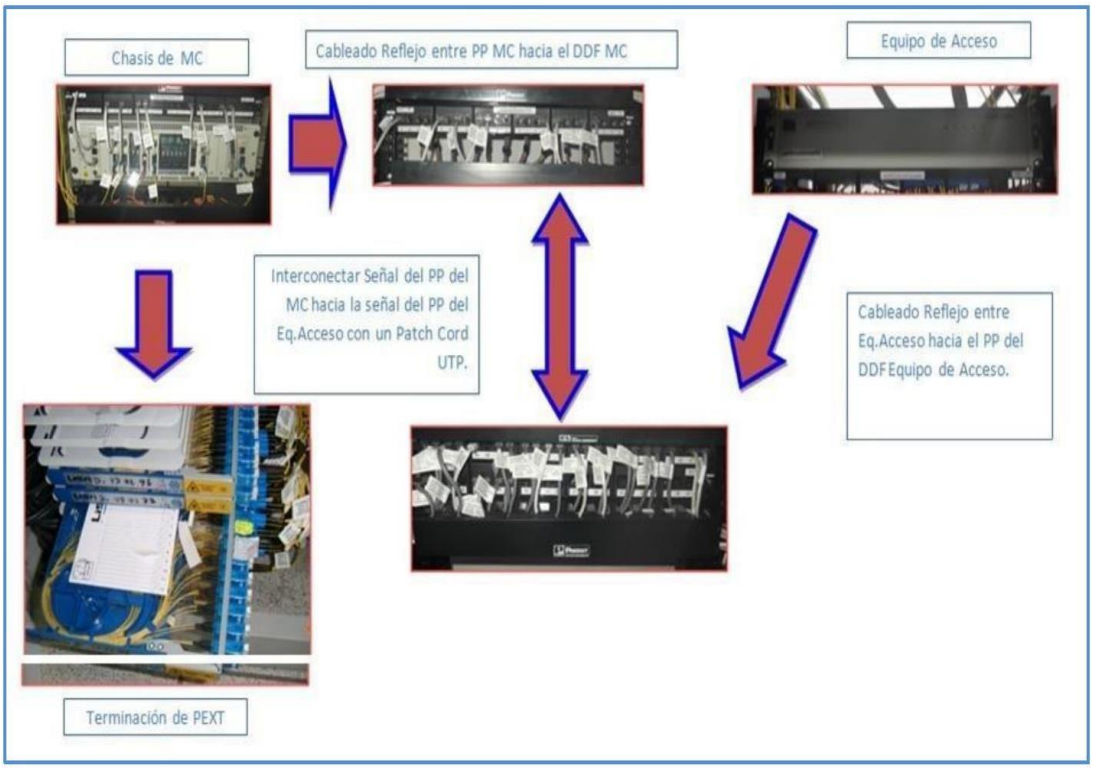
6. Etiqueta del Cable que une El Reflejo de reflejo Cmetro (DDF Equipo de Acceso) con el del MC (DDF UM):



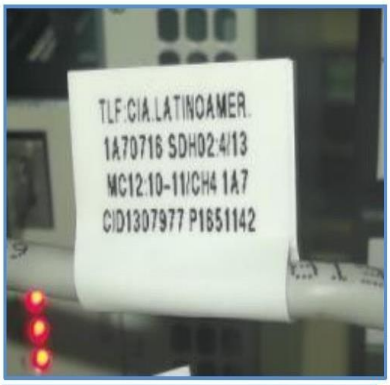
Etiqueta del Reflejo del Equipo de Acceso.
2da Línea – Destino: N°Rack, N°PP, N°PtoPP y N°MC:N°Slot. 3ra Línea – Origen: N°Rack, N°PP, N°PtoPP y Eq.Acc:Slot/Pto.

7. No se etiqueta en los cables instalados en el Equipo de Acceso.

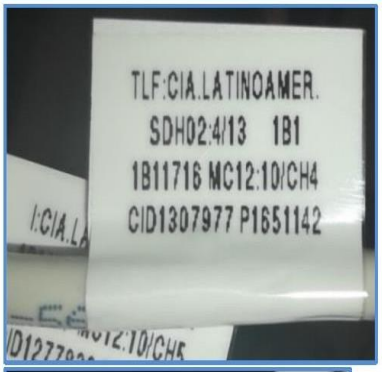
Diagrama de Conexión en Pop con cableados Reflejos - Primario:



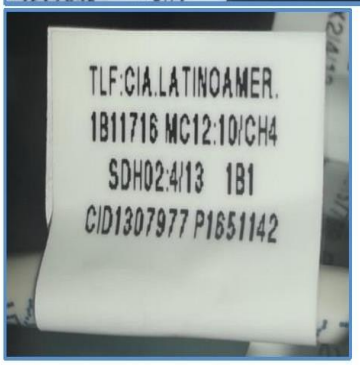
8. Para Servicios de Primario: En este caso contamos con una Tarjeta MC MUX, se considera el N° del Canal del E1, cuando es Tarjeta de 01 Slot, no se coloca el Canal.



Etiqueta en el Puerto RJ de la Tarjeta MC.
2da Línea – Destino: N°Rack, N°PP, N°PtoPP y y Eq.Acc:Slot/Pto. 3ra Línea – Origen: N°MC:N°Slot./N°Canal y N°Rack.



Etiqueta en el PP del MC
2da Línea – Destino: Eq.Acc:Slot/Pto y N°Rack. 3ra Línea – Origen: N°Rack, N°PP, N°PtoPP y N°MC:N°Slot./N°Canal.



Etiqueta en el PP del Equipo de Acceso
2da Línea – Destino: N°Rack, N°PP, N°PtoPP y N°MC:N°Slot./N°Canal. 3ra Línea – Origen: Eq.Acc:Slot/Pto y N°Rack.

Equipo de Acceso

ETIQUETADO EN EL LADO CLIENTE

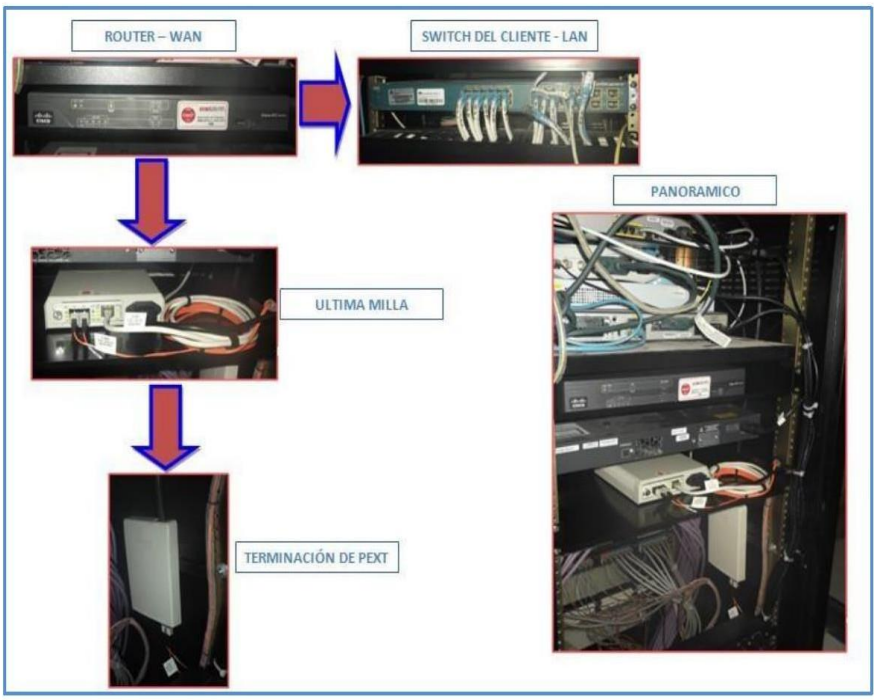
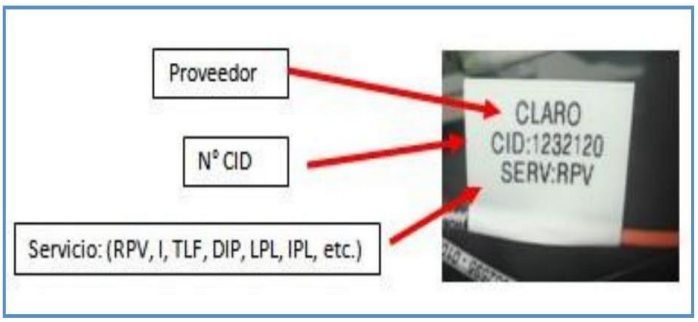


Diagrama de Conexión en el Cliente Datos:

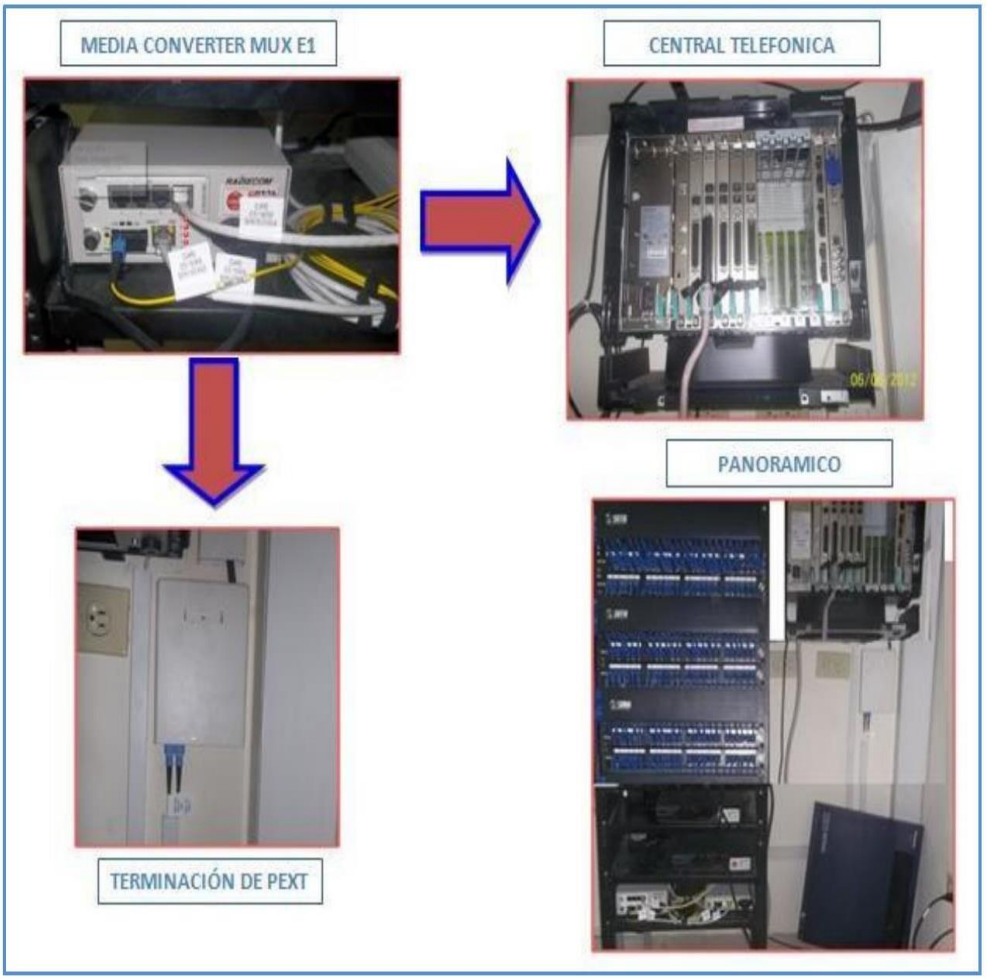
1. Solo Realizamos 04 Etiquetas del mismo modelo y formato:



2. 02 Etiquetas para el Jumper de Fibra (01 para cada extremo)

3. 01 Etiqueta para Patch Cord en MC y 01 Switch Lan del Cliente.

Diagrama de Conexión en el Cliente Datos:



SECUENCIA DE FOTOS

EN EL POP CON DDF

Nº DE ORDEN.		
1	Chasis MC	(Panorámico chasis: Raisecom, Transition)
2	Etiqueta FO MC	
3	Etiqueta CU MC	(Patch Cord 1 Feet)
4	Panorámico PP CU MC	(DDF del Chasis)
5	Etiqueta CU PP	(Origen MC – Destino Eq. acceso)
6	Panorámico PP CU EQ de Acceso	(DDF del Eq. Acceso)
7	Etiqueta CU PP	(Origen Eq. Acceso - Destino MC)
8	Panorámico PP EQ de Acceso	(Reflejo Directo del Eq. Acceso)
9	Panorámico EQ de Acceso	(CT:4506, 4503, 4948. 2900, RT:7200, Optix, M3100 Caja H, etc)
10	Panorámico Opticom FO	(Opticom, GCO, H&S, Caja Panduit, etc)
11	Etiqueta FO Opticom	

POP SIN CABLEADO REFLEJO O POR DE GRIFO:

Nº DE ORDEN.		
1	Chasis MC	(Panorámico chasis: Raisecom, Transition)
2	Etiqueta FO MC	
3	Etiqueta CU MC	(Origen MC – Destino Eq. acceso)
4	Panorámico EQ de Acceso	(CT:4948, 2900, RT:7200, Optix, M3100 Caja H, etc)
5	Eiqueta CU	(Origen Eq. Acceso - Destino MC)
6	Panorámico Opticom FO	(Opticom, GCO, H&S, Caja Panduit, etc)
7	Etiqueta FO Opticom	

EN EL CLIENTE:

Nº DE ORDEN.		
1	Panorámico de Router	
2	Panorámico de S.A.	
3	Panorámico de Router + S.A.	
4	Etiqueta FO	
5	Etiqueta CU	
6	Panorámico de Caja Panduit	(Opticom, GCO, H&S, Caja Panduit, etc)
7	Toma de Energía	
8	LAN Cliente	(Switch, Central Telefónica, etc. En el cual se note el cable etiquetado)

CONFIGURACIONES BASICAS DE ETIQUETADORA BROTHER

Etiquetadora BROTHER P -TOUCH
Configuración Básica
Etiquetado en Planta Interna Pop + Cliente
Con Etiquetas de 24mm 1"

Tipo de Etiqueta	
Label Type	Rotate
	BLK LEN. 30 mm

Configuración Principal	
	Setup
CUT	1
CONTRAST	0
AUTO REDUCTION	TEX WIDTH
LENGTH ADJUST	0
SYMBOL SAVE	ON
UNITS	mm
LENGUAGE	ENGLISH
VERSION INFO	MAIN : 1.07

Configuración De Formato	
	Style
STYLE NORMAL ó BOLD	ENTER
	Size
SIZE AUTO	
WIDTH NORMAL	ENTER

ó el botón Azul "Format"	
GLB SIZE AUTO	AA
GLB WIDE NORMAL	A
GLB STYL NORMAL ó BOLD	**A**

Borrar todo el texto	
	Clear
Ok TO CLEAR TEXT & FROMAT	Enter

CONFIGURACIONES BASICAS DE ETIQUETADORA BROTHER 2470

Etiquetadora BROTHER P -TOUCH 2470
Configuración Básica
Etiquetado en Planta Interna Pop + Cliente
Con Etiquetas de 24mm 1"

Tipo de Etiqueta	
Label Type	Rotado
	BLK LEN. 25 mm

Configuración Principal	
	Setup "Z"
CUT	1
CONT. PANTALLA	0
REDUC. AUTO.	ANCHO. TEXT
AJUST. LONG.	0
ACTUAL. SIMBOL.	ACTIVADO
UNIDAD	mm
IDIOMA	ESPAÑOL
INFO VERSION	PRINC:1.00

Configuración De Formato	
	Letra "D"
ESTILO NORMAL	ENTER
	Letra "E"
TAMAÑO AUTO	ENTER
ANCHO NORMAL	ENTER

Cambiar de Mayuscula a Minuscula	
	Shift
A - a	Enter

Insertar Simbolos	
Buscas : / - & % , etc	Se Graba Enter

Borrar todo el texto	
	Clear "X"
¿BORRAR? TEXTO y/o FORMATO	Enter