UNIVERSIDAD TECNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULO DE INGENIERO EN INFORMÁTICA

Auditoría de Seguridad Informática del Centro de Procesamiento de Datos de la empresa EDPACIF S.A; implementación de una aplicación Web para la administración de los elementos auditados.

TRABAJO DE FIN DE TITULACIÓN.

AUTOR: Muñoz Ramos, Edmundo Arturo

DIRECTORES:

Guamán Bastidas, Franco Olivo, M.Sc.

Quezada Sarmiento, Pablo Alejandro, M. Sc.

CENTRO UNIVERSITARIO – SANTO DOMINGO

2015

APROBACIÓN DEL DIRECTOR DE TRABAJO DE FIN DE TITULACIÓN

Master.
Pablo Alejandro Quezada Sarmiento,
DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de fin de titulación: “Auditoría de Seguridad Informática del Centro de Procesamiento de Datos de la empresa EDPACIF S.A; implementación de una aplicación WEB para la administración de los elementos auditados”, realizado por el profesional en formación Muñoz Ramos Edmundo Arturo; ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, Mayo 2015.

f) Quezada Sarmiento Pablo Alejandro
C.I: 1103863229

APROBACIÓN DEL DIRECTOR DE TRABAJO DE FIN DE TITULACIÓN

Master.
Franco Olivo Guamán Bastidas,
DOCENTE TRABAJO DE TITULACIÓN

De mi consideración:

El presente trabajo de fin de titulación: “Auditoría de Seguridad Informática del Centro de Procesamiento de Datos de la empresa EDPACIF S.A; implementación de una aplicación WEB para la administración de los elementos auditados” realizado por el profesional en formación Muñoz Ramos Edmundo Arturo; ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, Mayo 2015.

f) Guamán Bastidas Franco Olivo
C.I: 1102827977

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, Muñoz Ramos Edmundo Arturo; declaro ser autor del presente trabajo de fin de titulación: “Auditoría de Seguridad Informática del Centro de Procesamiento de Datos de la empresa EDPACIF S.A; implementación de una aplicación WEB para la administración de los elementos auditados”, de la Titulación de Ingeniería Informática, siendo los Msc. Quezada Sarmiento Pablo Alejandro y Msc. Guamán Bastidas Franco Olivo directores del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja, que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

f._____

Autor: Muñoz Ramos Edmundo Arturo

Cédula: 170763519-7

DEDICATORIA

A Dios, a mi familia, en especial a mi madre que me apoyo en todo momento y que no podrá estar conmigo en la culminación de esta meta; a mi esposa y a mis hijos que han sido un apoyo constante y me han alentado siempre a seguir adelante, superando las dificultades. A ustedes con cariño, por creer en mí.

A mis estimados y distinguidos facilitadores de la Universidad Técnica Particular de Loja que desde el inicio de esta carrera han puesto a mi disposición sus conocimientos, los mismos que se ven ahora plasmados en este trabajo. A todos ustedes muchas gracias.

Arturo

AGRADECIMIENTO

Mi agradecimiento profundo a Dios por permitirme culminar esta meta; a mi madre quién siempre me incentivó a seguir adelante y desde el cielo ve con orgullo la terminación de este ciclo.

A mi esposa Digna e hijos Carlos y Camila, que con su aliento y confianza me llevaron a culminar esta meta, sin su apoyo y comprensión no hubiera sido posible alcanzarla.

A mis directores de tesis: M.Sc. Pablo Alejandro Quezada Sarmiento y M.Sc. Franco Olivo Guamán Bastidas, por su acertada dirección, su tiempo, su apoyo en la revisión y por haber guiado en buena forma, la realización de este trabajo de investigación.

Arturo

INDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La auditoría se basa en el estudio de los componentes básicos que garantizan la seguridad de la información, de acuerdo al estándar Cobit 4.1.

Se desarrolló un banco de preguntas para cada componente, para obtener la información necesaria para la auditoria; esta se analiza para establecer el grado de cumplimiento con las normas internacionales y determinar los niveles de madurez y los niveles de riesgo de cada uno de los componentes analizados, con el fin de recomendar las acciones a ejecutar para minimizar el impacto que estas puedan causar al recurso información.

Para la automatización del proceso se desarrollo de una aplicación web, en la que se cargan las preguntas de las encuestas que se aplicaron, las respuestas, y las fechas de realización. Los resultados del análisis (hallazgos, efectos y recomendaciones) se ingresan a la aplicación. Esta información servirá para controlar el avance de la auditoria.

Tienen acceso a esta aplicación el auditor que es el encargado de ingresar la información a las bases de datos, y los usuarios a través de la dirección URL de la aplicación www.seguridadinformatica.esy.es/sitio4/index.php

PALABRAS CLAVES: seguridad, información, Cobit 4.1, niveles de madurez, niveles de riesgo, componentes, impacto, hallazgos, efectos, impacto, análisis.

ABSTRACT

The process audit is based on the study of the basic components that guarantee the security of the information, in accordance with the standard Cobit 4.1.

A Bank of questions for each component, was developed to obtain information necessary for the audit; This analysed to establish the degree of compliance with standards international and determine the maturity levels and the levels of risk of each of the components analyzed, in order to recommend actions to run to minimize the impact that these may cause to the information resource.

Automating the process was developed for a web application, in which questions of surveys that were applied, are charged responses, and completion dates. The results of the analysis (findings, effects and recommendations) are entered in the application. This information will be used to monitor the progress of the audit.

Tienen acceso a esta aplicación el auditor que es el encargado de ingresar la información a las bases de datos, y los usuarios a través de la dirección URL de la aplicación www.seguridadinformatica.esy.es/sitio4/index.php.

Keywords: security, information, Cobit 4.1, levels of maturity, levels of risk, findings, components, impact, effects, impact, analysis.

INTRODUCCIÓN

La seguridad informática ha tenido un gran avance en los últimos años, debido al desarrollo acelerado de nuevas condiciones y plataformas tecnológicas que presentan diferentes retos a los encargados de la seguridad de la información por el aumento constante de amenazas y nuevas formas de vulnerar la seguridad de los sistemas informáticos.

Piattini, M. (2008); explica que "*la realidad tecnológica impone un reto a las empresas; protegerse no solo del peligro de exponer sus operaciones, sino también las de sus clientes, proveedores, socios y empleados; reduciendo los problemas de seguridad, teniendo cuidado en dar a la información la importancia y valor como el activo más valioso que posee la organización*".

De acuerdo a Gómez, A. (2011); "*las tecnologías de la información, cada vez más necesarias para garantizar la competitividad del negocio nos plantean la pregunta sobre si está garantizada la confiabilidad y seguridad de los sistemas y productos informáticos en un medio que cada día es más dependiente de ellos*".

Como todas las áreas de la organización, los sistemas de tecnologías de información deben someterse a controles de calidad y auditoría, toda vez que estos y los centros de procesamiento de datos podrían ser blancos de ataques como: espionaje, terrorismo, venganza de empleados y ex empleados descontentos que intenten vulnerar los controles para conseguir información de la empresa, ocasionar daños a la información o simplemente obtener notoriedad.

Según Mujica, M. (2010), "*seguridad de la información es mucho más que establecer firewalls, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, o guardar en la bóveda los backups; seguridad de información es determinar qué hay que proteger, por qué, de qué se debe proteger y como protegerlo*."

Por ello auditoría informática debe enfocarse no solamente en los equipos de cómputo; sino en evaluar los sistemas partiendo de la información de entrada, procedimientos, controles, seguridad y almacenamiento de información; desde donde se determina la vital importancia de la auditoría informática para las empresas.

Para iniciar la auditoria se debe hacer una visita preliminar con la finalidad de recabar información que permita al auditor tener un conocimiento inicial de la empresa que va a auditar. El presente trabajo de titulación está estructurado en:

Capítulo I, presenta a la empresa EDPACIF S.A de manera general; detallando información sobre su historia, actividad a la que se dedica, ubicación, misión, visión, valores y estructura organizacional.

Capítulo II, trata sobre la metodología de desarrollo, determinando alcance y objetivos, estudio inicial del entorno auditable, forma de recopilar la información y el análisis de los datos recopilados. Se presenta la normativa utilizada para realizar la auditoria basada en el estándar (Cobit 4.1) y una explicación de los componentes a auditar con sus respetivos elementos.

En el capítulo III, se presenta la información recolectada a través de los formatos de entrevista aplicados a los responsables del CPD, formatos preparados para cada componente a auditar (Anexos 2-7).

El capítulo IV se procede al análisis de la información recolectada, y se presenta el modelo genérico de madurez de Cobit 4.1, las matrices de: determinación de impacto, probabilidad de ocurrencia y evaluación de riesgos; las mismas que serán utilizadas para cada dominio y procesos de Cobit; así como para cada componente y sus elementos.

En el capítulo V se muestra el proceso de desarrollo de la aplicación Web: visión del proyecto, descripción global del producto, sistema a desarrollarse, restricciones, requisitos del sistema, requerimientos. También presenta el plan de desarrollo de software, plan de fases, arquitectura y diagramas de caso uso, modelo de dominio, diagrama de clases, diagramas de datos, diagramas de secuencia, diagramas de colaboración, diagramas de estado, diagrama de implementación, prototipos de interfaz de usuario.

El capítulo VI presenta las conclusiones obtenidas del análisis previo, así como las recomendaciones que permitan corregir los problemas detectados en la auditoria de seguridad de la información al centro de procesamiento de datos de la empresa Edpacif SA.

CAPÍTULO I.
ASPECTOS GENERALES DE LA EMPRESA EDPACIF S.A.

1.1. Historia.

Empacadora del Pacífico “EDPACIF S.A”, fue creada con la visión de satisfacer las necesidades de sus clientes y al mismo tiempo colaborar con el desarrollo socio-económico del sector de Coaque y Pedernales.

La empacadora inicio sus operaciones en el año 2001 dando como resultado su primera exportación en marzo del mismo año. “EDPACIF S.A” consiguió la certificación HACCP (Hazard Analysis and Critical Control Point) en el año 2002, lo que asegura un control de los puntos críticos en el procesamiento del camarón e incluye la trazabilidad del producto empacado en todas las operaciones de producción y comercialización. Está implementando actualmente el sistema de gestión BRC versión 6 (British Retail Consortium) que es un sistema de seguridad alimentaria, esta es una norma específica para la industria agroalimentaria, siendo sólo aplicable a compañías fabricantes o envasadoras de productos alimenticios.

Una de las fortalezas de “EDPACIF S.A” que perdura desde sus inicios hasta la actualidad es que sus productos son una marca reconocida a nivel internacional por su calidad, inocuidad y legalidad, mediante el cumplimiento de los requisitos de sus clientes, lo cual ha generado una gran relación de confianza y el mantenimiento de clientes a largo plazo.

1.2. Ubicación.

La Planta Procesadora de Empacadora del Pacífico “EDPACIF S.A” está ubicada en la línea ecuatorial cerca de la ciudad de Pedernales en el sitio Coaque, Ecuador (Km 9 1/2 Vía Pedernales San Vicente).

Única empacadora en la mitad del mundo (A 1 km de la línea ecuatorial). Está rodeada por aguas limpias del Océano Pacífico y de un hermoso paisaje rural. Su cercanía a los estuarios de Cojimíes, Jama, Muisne y Bahía de Caráquez le permite a “EDPACIF S.A” acceder a una zona de producción de alrededor de 20 mil hectáreas.

Por su localización estratégica, el camarón que llega a la planta es procesado en muy poco tiempo, permitiendo entregar a sus clientes productos de alta calidad y frescura.

Figura 1. Ubicación de Empacadora del Pacífico S.A. Adaptado de Google Inc. https://maps.google.com.ec/maps?hl=es-419tab=wl

1.3. Misión.

Empacadora del Pacífico “EDPACIF S.A”, procesa camarones cultivados en cautiverio, utilizando técnicas adecuadas de control de calidad, procesos y trazabilidad, que aseguran la inocuidad de nuestros productos, cumpliendo con los requisitos implícitos y explícitos de nuestros clientes.

1.4. Visión.

Lograr el liderazgo de la producción camaronera ecuatoriana, en base a procesos eficientes y seguros para cumplir con las exigencias legales y de calidad de nuestros clientes, contando con personal capacitado, e innovando constantemente los productos y procesos.

1.5. Valores.

- Cumplimiento con nuestros convenios.
- Transparencia y ética en todos nuestros actos.
- Relaciones a largo plazo con nuestros proveedores y clientes.
- Desarrollo y beneficio mutuo con nuestros colaboradores.
- Intolerancia al desperdicio.
- Obsesión por la calidad.
- Mejoramiento continuo.

- Actualización tecnológica en todos nuestros proceso.

1.6. Estructura

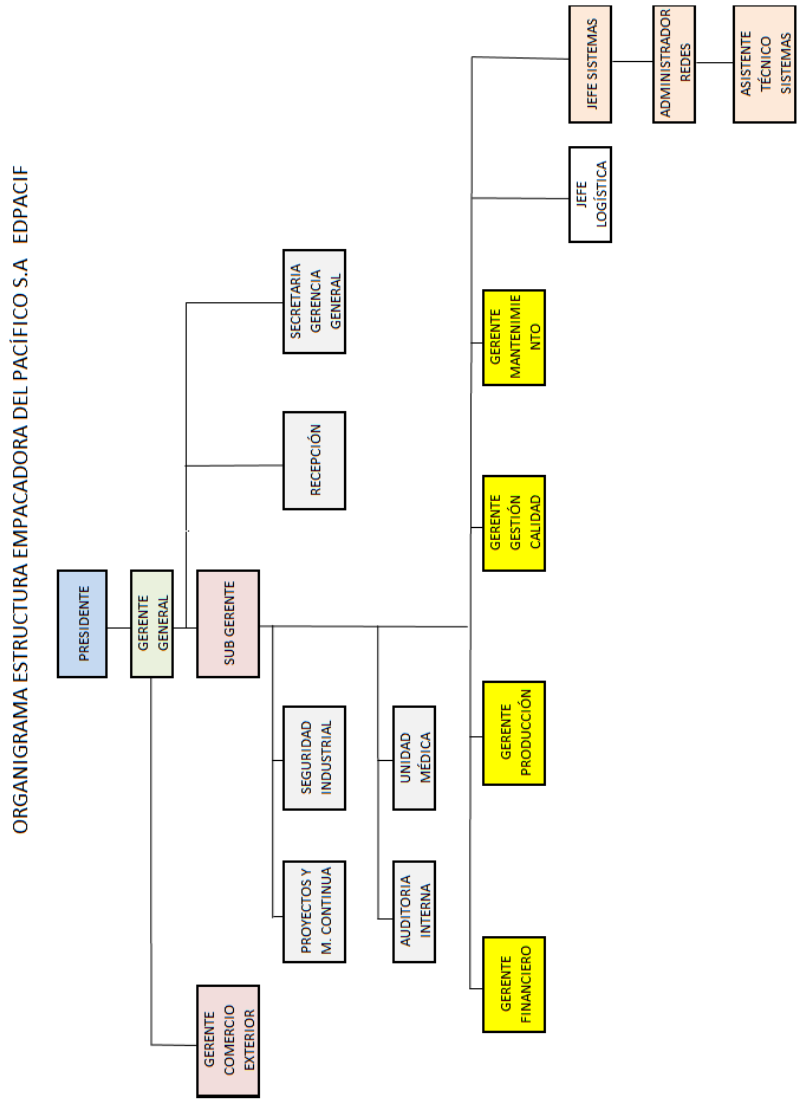


Figura 2. Organigrama Estructural EDPACIF. Edpacif Auditoría Interna (2014).

CAPÍTULO II.
AUDITORÍA DE LA SEGURIDAD

2.1. Desarrollo de la Auditoria.

Para el presente trabajo se necesita adoptar un proceso de desarrollo **cualitativo**: basado en la determinación de la calidad de los controles y **subjetiv**o: apoyado y basado en el criterio técnico y experiencia del auditor; utilizando normas y procedimientos establecidos en el estándar internacional Cobit 4.1, aplicado a los diferentes componentes a auditar; para esto se utilizó los pasos básicos para el desarrollo de una auditoría:

- Determinar el Alcance y Objetivos de la Auditoría
- Recopilación de información.
- Estudio inicial del entorno auditable.
- Análisis de la información recopilada**.**
- Conclusiones y Recomendaciones.

2.1.1 Alcance la Auditoría

Alcance.

La auditoría propuesta comprende el desarrollo y el estudio de los siguientes componentes:

- Seguridad Física
- Seguridad Lógica
- Seguridad de la Red
- Seguridad de las Aplicaciones
- Evaluación de la Administración del CPD
- Evaluación del Plan de Seguridad Informática

2.1.2 Objetivos de Auditoría

Objetivo General.

Realizar una Auditoría Informática del centro de procesamiento de datos e implementación de un sistema web que facilite administrar los componentes auditados, con el fin de conocer vulnerabilidades de los controles, políticas, planes y procedimientos de Seguridad.

Objetivos Específicos:

- Conocer la situación de la información en cuanto a protección, control y medidas de seguridad.
- Verificar el nivel de cumplimiento de los controles, políticas y procedimientos establecidos con el estándar Cobit.
- Establecer en base al estándar Cobit el nivel de madurez en que se encuentra la organización en los diferentes componentes auditados.
- Determinar el nivel de riesgo a que está expuesta la información de acuerdo a los componentes auditados.
- Proponer los correctivos necesarios para cada elemento auditado, de manera que se alcance los objetivos fundamentales de la Gestión de la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad.

2.1.3 Estudio inicial del entorno auditable.

En esta actividad se requiere una visita a la empresa o institución donde se realizará la auditoría con la finalidad de conocer su personal, observar el número de equipos instalados, distribución de los mismos y los sistemas de protección y control de acceso. En el estudio inicial se pretende conocer:

- Organigrama.- Que es la representación gráfica de la estructura de la organización.
- Departamentos.- Son las áreas de la empresa estructuradas de acuerdo a sus funciones y que dependen de la dirección, ejemplo (Departamento de Sistemas, Departamento Financiero).
- Relaciones Jerárquicas y funcionales entre órganos de la empresa.- Relaciones de autoridad, subordinación , control y relaciones funcionales previstas en el organigrama
- Flujos de Información.- Además de las relaciones verticales jerárquicas directas entre departamentos, la estructura de la organización mantiene un intercambio de información horizontal y oblicua entre estos.

- Puestos de trabajo.- Los nombres de los puestos de trabajo corresponden a las funciones reales.
- Entorno Operacional.- la situación geográfica de los distintos centros de procesamiento de datos, responsables, la arquitectura y configuración de hardware y software de los equipos; inventario de hardware y software, bases de datos, metodologías de diseño.

2.1.4 Recopilación de información.

La recopilación de la información pretende mediante entrevistas con el personal responsable de las diferentes áreas del CPD, conocer los procedimientos, actividades y controles internos utilizados para garantizar la integridad, confidencialidad y disponibilidad de la información, con este propósito se diseñó encuestas para recabar información de los siguientes aspectos:

- Seguridad Física.
- Seguridad Lógica.
- Seguridad de la Red.
- Seguridad de las Aplicaciones.
- Evaluación de la Administración del CPD.
- Evaluación del Plan de Seguridad.

Las encuestas fueron elaboradas de tal manera que permitan recopilar información relevante sobre los procesos y actividades que se llevan a cabo en la empresa con la finalidad de garantizar la seguridad en los diferentes aspectos antes expuestos. (Visualizar Anexos 2-7)

2.1.5 Análisis de la información recopilada.

Con la información obtenida en la etapa anterior, se procedió a analizar la misma y compararla con los estándares internacionales a fin de establecer el nivel de cumplimiento y realizar ajustes a los mismos para garantizar la seguridad del recurso información.

De cada aspecto a auditar se analiza si las actividades de seguridad que se llevan a cabo actualmente en la empresa se ajustan a las normas y estándares internacionales y cumplen a satisfacción su objetivo. Con este análisis se pretende determinar el grado de exposición de la información a potenciales riesgos que comprometan la integridad, confidencialidad y

disponibilidad de la información; a la vez se establece las recomendaciones pertinentes para cubrir estas debilidades.

2.2. Normativa utilizada Cobit 4.1.

Para la realización de la auditoria se utiliza el estándar Cobit 4.1 2007, que es un estándar generalmente aplicado y aceptado mundialmente para el control de tecnologías de información, el cual está basado en los objetivos de control del Information System Audit and Control Foundation. Cobit es desarrollado por un grupo internacional de expertos y revisores, cuenta entre sus afiliados y patrocinadores a importantes instituciones del ámbito informático a nivel mundial como: ISACA, ITGI Japón, Information Security Forum, The Informatión Systems Security Association, Commowealth Asociation of Corporate Governance, entre otros.

Para él Gobernance Institute (2007); los objetivos de control para la Información y Tecnología relacionada brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentan las actividades en una estructura manejable y lógica. Las buenas prácticas de CobiT 4.1 (Control Objectives for Information and related Technology) representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, aseguran la entrega y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados.

Normalmente se ordenan dentro de dominios de responsabilidad del plan, construir, ejecutar y monitorear. Dentro del Marco de Cobit, el IT. Gobernance Institute (2007), establece los siguientes dominios:

Tabla 1.

Dominios de Cobit 4.1.	
Dominio	**Descripción**
Planear y Organizar (PO)	Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicios (DS).
Adquirir e Implementar (AI)	Proporciona las soluciones y las pasa para convertirlas en servicios.
Entregar y Dar Soporte (DS)	Recibe las soluciones y las hace utilizables por los usuarios finales.
Monitorear y Evaluar (ME)	Monitorear todos los procesos para asegurar que se sigue la dirección correcta.

Fuente: Adaptado IT. Gobernance Institute Cobit 4.1 2007.- *Marco de Trabajo, Objetivos de Control, Directrices Generales, Modelos de Madurez.*

2.2.1 Planear y organizar (PO).

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio? (IT. Gobernance Institute, 2007, p.29).

2.2.2. Adquirir e implementar (AI).

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Es probable que los nuevos proyectos generen soluciones que satisfagan las necesidades del negocio?
- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez que sean implementados?
- ¿Los cambios no afectan a las operaciones actuales del negocio?
  (IT. Gobernance Institute, 2007, p.73).

2.2.3. Entregar y Dar Soporte (DS).

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas. Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

(IT. Gobernance Institute, 2007, p.101)

2.2.4. Monitorear y Evaluar (ME).

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar problemas antes de que sea demasiado tarde?
- ¿La gerencia garantiza que los controles internos sean efectivos?
- ¿Puede vincularse el desempeño que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

(IT. Gobernance Institute, 2007, p.153).

En IT. Gobernance Institute (2007), se divide a CobiT en un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear.

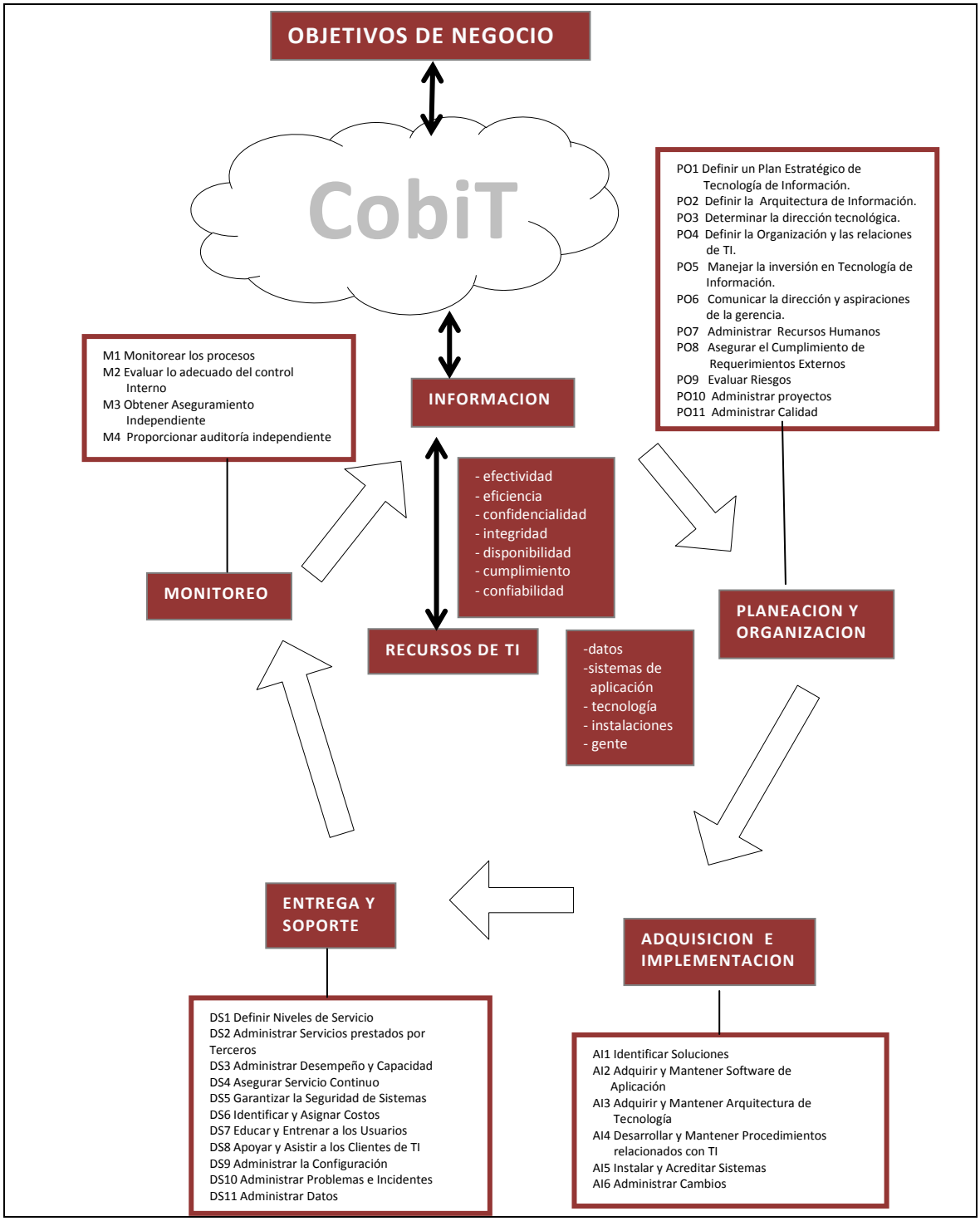


Figura 3. Procesos definidos dentro de los Cuatro Dominios de TI. IT. Gobernance Institute Cobit 4.1 2007.

2.3. Seguridad física.

De acuerdo a Gómez, A. (2011), "*la seguridad física es la implementación de barreras materiales y mecanismos de control en un ambiente informático, de manera que se pueda garantizar la integridad, confidencialidad y disponibilidad de la información. La seguridad física tiene que ser complementada con la seguridad lógica*." Comprende evaluar que en el centro de procesamiento de datos, los dispositivos, los equipos, medios de almacenamiento y personas cumplan con las medidas de seguridad referentes a la infraestructura física y seguridad de los recursos de la institución.

Es muy importante comprender claramente que por más que estemos protegidos contra ataques externos tales como: hackers, virus, entre otros; la seguridad de una empresa será nula si no se ha previsto como enfrentar un desastre natural y/o un ataque interno.

Las actividades, mecanismos y controles de seguridad física deben proteger al hardware de amenazas generadas por el hombre así como por el ambiente. Las amenazas físicas que pueden comprometer y poner en riesgo un sistema informático son:

- Desastres naturales, incendios accidentales, humedad e inundaciones.
- Amenazas ocasionadas involuntariamente por personas.
- Acciones hostiles deliberadas como robo, fraude o sabotaje.

Entre los mecanismos de seguridad física que se podrán implementar tenemos:

- Cerrar con llave el centro de cómputo.
- Instalar extintores de incendios.
- Instalación de cámaras de seguridad.
- Dotar de Guardia de seguridad.
- Control permanente del sistema eléctrico, de ventilación, etc.

2.3.1. Equipamiento.

Conocer el tipo, cantidad y características del hardware instalado en la empresa; esto es servidores, PC's, módems, routers, entre otros.

Para Gómez, A. (2011), el computador al estar conectado a una red no puede ser considerado un elemento aislado, si consideramos al computador como un elemento

individual; tres elementos esenciales tenemos que analizar para evitar agujeros de seguridad:

- Evitar accesos locales al equipo por parte de personas no autorizadas.
- Evitar la contaminación del equipo por elementos que puedan producir daños o reducir la velocidad de funcionamiento del mismo, estos se instalan en los elementos de almacenamiento portátiles (USB, tarjetas SD, discos duros portátiles) y en los sistemas de comunicación para contaminar el equipo.
- Mantener actualizado el equipo informático, su sistema operativo y los programas que utilicemos, para evitar agujeros de seguridad.

En cuanto a evitar los accesos locales, la mayoría de los ataques se basan en la técnica llamada “Ingeniería social”.

En Gómez, A. (2011), se explica que:

- En los dispositivos como routers y módems que permiten acceso a los equipos y redes se puede aprovechar ciertas vulnerabilidades de estos para realizar fácilmente ataques a las redes conectadas a estos dispositivos.

- Las cámaras WEB y servidores de vídeo poseen fallos que permitirían el control remoto de la cámara propiciando un ataque de Denegación de Servicio (DoS).

- Los escáneres, fax e impresoras conectadas a una red, sin las protecciones adecuadas podrían facilitar la sustracción de información reservada o funcionamiento incorrecto del dispositivo entre otros problemas.

2.3.2. Control de acceso físico al CPD.

Gómez, A. (2011), indica que se debe determinar si existen los mecanismos y procedimientos de control de acceso a las instalaciones de la empresa, restricciones de acceso por tiempo, área o sector; estos procedimientos deben contemplar la definición de las siguientes áreas:

- Áreas Públicas: Lugares donde pueden acceder sin restricciones personas ajenas a la organización.
- Áreas Internas: Lugares reservados exclusivamente a los empleados

- Áreas de Acceso Restringido: Zonas críticas a las que sólo está permitido acceder a un grupo de empleados con un nivel de autorización definido.

Se debe definir cómo se va a identificar al personal de la empresa y cómo al personal ajeno a la misma, además la empresa debe mantener una lista actualizada del personal con autorización de acceso a las áreas críticas, así también una lista con los nombres de las personas visitantes.

Debe mantener un listado de los empleados que acceden a la empresa en horarios fuera de trabajo, así como un registro de entradas y salidas del personal, poniendo especial énfasis en los accesos a áreas restringidas.

2.3.3. Control de acceso a los equipos.

Determinar la existencia de procedimientos para restringir el acceso a equipos y dispositivos a personal no autorizado; de acuerdo a Gómez, A. (2011), para la protección física de los equipos, como los servidores y otros dispositivos, deberán ser ubicados en espacios acondicionados especialmente, con puertas que tengan cerraduras de seguridad, permitiendo el acceso con llaves, tarjetas electrónicas, equipos biométricos, implementando medidas de seguridad adicionales en días y horarios fuera de trabajo. Se tiene que tener un cuidado especial en la protección y configuración de los servidores, donde se debe contemplar aspectos como:

- Utilización de una contraseña a nivel de BIOS.
- Utilización de contraseñas de encendido del equipo.
- Ubicación de los servidores en salas con acceso restringido y otras medidas de seguridad física.
- Separación de los servicios críticos.
- Configuración robusta y segura de los servidores: desactivar las cuentas de usuario que no se van a utilizar, desactivar los servicios básicos, etc.
- Para reforzar las medidas de seguridad física se puede fijar los equipos a las mesas de trabajo; bloquear los lectores de CD/DVD y puertos USB, etc.

2.3.4. Dispositivos de almacenamiento.

En Piattini, M (2008), se explica que se debe determinar los procedimientos de control de los dispositivos para almacenamiento de información, se almacenan en un lugar adecuado y seguro, se mantiene inventarios, etc.

Para el control de los dispositivos de almacenamiento Piattini, M. (2008); determina que se debe disponer de un inventario actualizado de los soportes donde se guardan los datos e información sensible, estos soportes deben ser almacenados en lugares con acceso restringido, con la finalidad de evitar que otras personas puedan obtener dichos soportes.

El lugar donde se almacenan los soportes de información debe cumplir con las condiciones ambientales recomendadas por el fabricante, se debe contar con un registro de entradas y salidas de soportes; en el caso de soportes que contengan datos sensibles o de carácter personal se debe contar con la autorización de un funcionario responsable del área informática, esto debe ser debidamente documentado incluyendo fecha de salida, quién autorizó, a quién se envía.

2.3.5. Edificio.

El local destinado a albergar el CPD, debe cumplir con los requerimientos mínimos de seguridad que minimicen los riesgos que puedan producirse de forma intencionada o accidental; medidas como: características de construcción, control de acceso, vigilancia entre otros; Gómez, A. (2011), explica que se debe conocer los requisitos mínimos de seguridad para albergar un CPD, esto es en lo relacionado con protección frente a daños por fuego, inundación, explosiones, accesos no autorizados.

Selección de los elementos estructurales internos: puertas, paredes, pisos y techos falsos, canalizaciones de comunicaciones, eléctricas, entre otras. Definición de áreas o zonas de seguridad, zonas de carga, descarga y almacenamiento de suministros.

Sistemas de vigilancia: cámaras, detectores de movimiento, alarmas, etc. Control de condiciones ambientales: ventilación, aire acondicionado, calefacción, equipos de humidificación y des humidificación, entre otros.

2.3.6. Cableado.

Evaluar el tipo de cableado, diagramas de cableado, mantenimiento del cableado, conectores, etc. Para construir el cableado de las redes locales se utiliza desde el cable telefónico normal, cable coaxial hasta la fibra óptica, cada tipo de cable tiene sus propios problemas y desventajas. Según Gómez, A. (2011) los riesgos más comunes se resumen en:

- Interferencia: Pueden estar generadas por cables de alimentación de maquinaria pesada, campos eléctricos, equipos de radio y microondas.
- Corte de cable: La conexión se rompe lo que ocasiona se interrumpa el flujo de datos por el cable.
- Daños en el cable: Los daños en el cable generan el deterioro en el apantallamiento que protege la integridad de los datos transmitidos, produciendo la pérdida de fiabilidad de la información.

Estos problemas pueden atribuirse a daños naturales, sin embargo el cableado de red ofrece una nueva oportunidad para un atacante que desee acceder a la información de la organización. Esto se lo podría hacer:

- Desviando o estableciendo una conexión no autorizada.
- Haciendo una escucha sin hacer ninguna conexión.

Todos estos riesgos se deben minimizar con las adecuadas medidas y procedimientos tales como:

- Instalando cableado de Alto Nivel de Seguridad.
- Pisos de placas extraíbles, donde se aloja el cableado.
- Sistema adecuado de Aire Acondicionado.
- Filtro adecuados para control de emisiones electromagnéticas.

2.4. Seguridad lógica.

Mattos, E. (2010), hace referencia a un viejo dicho en seguridad informática que dicta que todo lo que no está permitido debe estar prohibido y esto es lo que debe asegurar la Seguridad Informática.

La Seguridad Lógica es la manera de aplicar procedimientos que aseguren que sólo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo; consiste en los controles y barreras de acceso a los sistemas de información y los datos que mantienen los Sistemas de Información, con la finalidad de detectar problemas que impidan se cumpla con los objetivos de la seguridad de la información: confidencialidad, disponibilidad, integridad; y así determinar las mejoras a implementar.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

- Cambio de los datos antes o cuando se le da entrada a la computadora.
- Copias de programas y /o información.
- Código oculto en un programa
- Entrada de virus

En el recurso web de Portillo K, (2014), se indica que "*La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas*."

Un método eficaz para proteger sistemas de computación es el software de control de acceso. El software de control de acceso protege contra el acceso no autorizado, al solicitar una contraseña antes de permitir el acceso a información confidencial.

2.4.1. Identificación y autenticación.

Para Gómez, A. (2011), la organización debe contar con una lista actualizada de usuarios autorizados, que tienen acceso a los recursos de los Sistemas de Información; para lo cual se debe tener determinados procedimientos de identificación y autenticación.

La identificación es el proceso por el cual el usuario presenta una determinada identidad para acceder al sistema. La autenticación de usuarios constituye uno de los elementos del modelo de seguridad conocido como "AAA" (Authentication, Authorization y Accounting) Autenticación, Autorización y Contabilidad.

- Autenticación es la validación de la identidad del usuario.
- Autorización acceso a los recursos del sistema basado en los permisos y privilegios de los usuarios.

Contabilidad es el proceso de registro del uso de los recursos del sistema por parte de los usuarios y de las aplicaciones (logs del sistema).

2.4.2. Roles.

Es importante que la organización cuente con algún procedimiento para establecer las operaciones que le está permitido realizar a cada usuario dentro del sistema de información, el objetivo es evitar que un usuario por accidente o de forma premeditada pueda realizar

operaciones que comprometan seriamente la integridad y el funcionamiento del SI. Los roles más comunes son:

Tabla 2.

Operaciones permitidas a los usuarios	
ROL	**FUNCIONES**
Administrador	Puede acceder a cualquiera de los aspectos del sistema, configurando o modificando cualquier parámetro de éste. Este usuario tiene control total sobre el SI, es decir está autorizado para realizar cualquier operación de configuración o mantenimiento
Usuario	Se le permite el acceso a ciertas aplicaciones del SI de acuerdo a sus funciones, no le está permito configurar o modificar el SI

Fuente: Adaptado Mattos, E. (2010). *Seguridad en el comercio electronico. Tesis Digitales UNMSM*.

2.4.3. Transacciones.

Establecer controles a través de las transacciones dependiendo del tipo de usuario, del grupo al que pertenece, solicitando el ingreso de una clave al requerir el procesamiento de una transacción determinada. Otras medidas de seguridad que garantizan la integridad de las transacciones son:

- Autenticación.
- Antivirus.
- Cifrado.
- Firewalls.

2.4.4. Limitaciones a los servicios.

Estos controles se refieren a las restricciones que dependen de medidas establecidas por el administrador o propias de la utilización de una aplicación. Por ejemplo licencias que restrinjan su uso a un número limitado de computadores.

2.4.5. Modalidad de acceso.

Se debe establecer el modo en que se permite el acceso al usuario a los recursos del SI; estos pueden ser:

- Lectura, el usuario puede solamente leer y ver la información, pero no puede modificarla, incluye el permiso de impresión.
- Escritura, este permiso permite agregar datos, modificar y borrar información.
- Ejecución este permiso otorga al usuario la capacidad de ejecutar programas.
- Borrado permite la eliminación de recursos del sistema.

2.4.6. Ubicación y horario.

De acuerdo a Piattini, M. (2008), la ubicación física o lógica de los datos o de la personas puede servir para fijar el acceso a determinados recursos del sistema. El horario permite limitar el acceso al SI a determinadas horas del día o determinados días de la semana, todo esto con la finalidad de mantener un control más restringido de los usuarios.

En algunos sistemas de información la recepción de datos de entrada y distribución de la salida debe obedecer a un horario elaborado con el usuario. Se debe también establecer horarios de trabajo en áreas sensibles de la empresa por lo que se elaborará un registro con los nombres de los empleados, el horario del turno y a que aplicaciones del SI tienen acceso durante su jornada de trabajo.

2.4.7. Control de acceso interno.

Se refiere a los controles para mantener la autenticación del usuario así como la inviolabilidad de la información; los passwords o palabras claves, sirven para la autenticación del usuario, generalmente el usuario elije para el password palabras fáciles de recordar lo que origina que estos sean débiles y fácilmente deducibles, para evitar este inconveniente se debe implementar mecanismos como:

- Sincronización de passwords que consiste en permitir que un usuario acceda con el mismo password a diferentes aplicaciones o sistemas interrelacionados; para evitar la dificultad que tienen los usuarios de recordar varias claves, lo que los lleva a escribirlas incrementado el riesgo de vulnerar los sistemas.
- Caducidad y control, este mecanismo controla cuando se puede y/o deben ser cambiados los passwords por los usuarios. Para esto se debe establecer el tiempo mínimo que debe transcurrir para que el usuario pueda cambiar su clave y el tiempo máximo que debe transcurrir para que los passwords caduquen.
- Es conveniente la encriptación de la información de tal manera que solo pueda ser desencriptada por la persona que tiene la clave; de igual forma se debe mantener una lista de control de accesos donde se encuentran los nombres de los usuarios, los permisos de acceso y la modalidad de acceso permitido. Otro mecanismo que se utiliza es establecer límites sobre la interfaz de usuario que básicamente son de tres tipos: menús, vistas sobre la base de datos y límites sobre la vistas de usuario.

2.4.8. Control de acceso externo.

Dispositivos de control de puertos.- Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar separados o incluidos en otro dispositivo de comunicaciones.

Firewalls o puertas de seguridad.- bloquean o filtran el acceso entre dos redes, permiten que los usuarios internos se conecten a la red exterior, proveyendo al mismo tiempo de protección contra atacantes o virus.

Acceso de personal contratado o consultores.- debe ponerse especial atención en la política y administración de sus perfiles de acceso ya que este personal presta servicios temporales.

2.4.9. Administración de personal.

Piattini, M. (2008); ha de establecerse procedimientos para la Administración del Personal y Usuarios el mismo que debe contemplar:

- Organización del personal.
- Definición de puestos.- considerar la máxima separación de funciones y el otorgamiento del mínimo permiso de acceso requerido por cada puesto.
- Determinación de la sensibilidad del puesto.- determinar si la función requiere permisos riesgosos.
- Elección de la persona para cada puesto.- considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto.
- Entrenamiento inicial y continuo.- el empleado debe conocer las disposiciones organizacionales y su responsabilidad en cuanto a la seguridad informática.

2.5. Seguridad de la red.

Gómez, A. (2011), evaluar los controles implementados para garantizar la seguridad de las comunicaciones, de los datos transmitidos, las conexiones remotas y los sistemas utilizados para la transmisión, analizando si cumplen con las normas y regulaciones de seguridad de la información, los puntos a analizar son:

- Evaluar si la organización cuenta con un inventario actualizado de los elementos que conforman la red, cuenta con un gráfico de la red que da servicio a la institución. De igual manera conocer con que filtros cuenta cada uno de los dispositivos y si existe encriptación a nivel de hardware.

- Qué características tiene los servidores, que parámetros se tomaron en cuenta para elegir el servidor de hosting, medidas de seguridad, respaldos de emergencia en caso de caída del servidor, entre otras.
- Características del módem, los datos se encriptan, se realiza los controles adecuados en la comunicación, etc.
- Se deshabilitaron los puertos que no son necesarios, cuáles y de que protocolos y servicios, quién es el encargado, se realizan pruebas de autohaqueo, etc.
- Se ha considerado la implantación de medios alternativos de transmisión de datos en caso de emergencia.
- Se utiliza alguna herramienta para administrar el correo y como se hace, está configurada adecuadamente.
- Se hace periódicamente un chequeo de la red y sus permisos, se mantiene una documentación de estos.

2.5.1. Topología de la red.

Estebañez, M.; Ibañez, M. & Manzano, A. (2012), establecen tres aspectos diferentes a la hora de considerar una topología:

- La topología física, que es la disposición real de los host y de los cables (los medios) en la red.
- La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).
- La topología matemática, donde los mapas de nodos y los enlaces a menudo forman patrones.

Aguirre, X. (2001) "*en la topología de broadcast cada host envía sus datos hacia los demás hosts de la red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet. La transmisión de tokens controla el acceso a la red al transmitir un token de forma secuencial a cada host. Cuando un host recibe el token, este puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir*".

El término topología en redes se refiere a la forma en que los computadores están organizados, cables y otros componentes de la red, la elección de la topología adecuada tendrá un impacto sobre:

- El tipo de equipo que la red necesita
- Las capacidades de este equipo
- Desarrollo de la red
- La forma en que la red es manejada

Para que las computadoras puedan compartir archivos y poder transmitirlos debe haber una correcta comunicación entre ellas. La mayoría de las redes usan un sistema físico para la intercomunicación, sin embargo no es solo conectar terminales a través de un sistema de cables. Existen diferentes configuraciones conocidas como, topologías las cuales se detallan a continuación; las cinco topologías básicas son:

2.5.1.1. Topología en bus.

Según Tanenbaum, A. (2003), en esta topología las computadoras están conectadas por un canal de comunicación denominado backbone. Esta red es la más común y la más simple.

Figura 4. Topología en Bus, las computadoras se conectan en línea recta. Adaptado. Universidad Autonoma de México (sf). Administración de Redes http://redyseguridad.fi-p.unam.mx/proyectos/asmonredes/PHP/capitulo1.html

Solo una computadora a la vez puede mandar mensajes en esta topología, por esto, el número de computadoras conectadas al bus va a afectar el rendimiento de la red.

Tabla 3.

Topología en Bus, ventajas y desventajas	
VENTAJAS	**DESVENTAJAS**
Fácil de añadir estaciones de trabajo	Disminuye el tiempo de acceso según el número de estaciones.
Maneja grandes anchos de banda	Si existe gran cantidad de equipos conectados el tiempo de respuesta es más lento
Muy económica	Presenta poca inmunidad al ruido
Soporta de decenas a centenas de equipos	Las distorsiones afectan a toda la red
Software de fácil manejo	Como hay un solo canal, si este falla, falla toda la red
Sistema de simple manejo	Es posible solucionar redundancia

Fuente: Adaptado de Tanenbaum, A. (2003)

2.5.1.2. Topología en estrella.

Gil P., Pomares J. y Candelas, J. (2010); indican que en esta topología los cables de todas las computadoras son conectados a un dispositivo central llamado hub, el mismo que transmite los datos de una computadora al resto de las computadoras en la red.

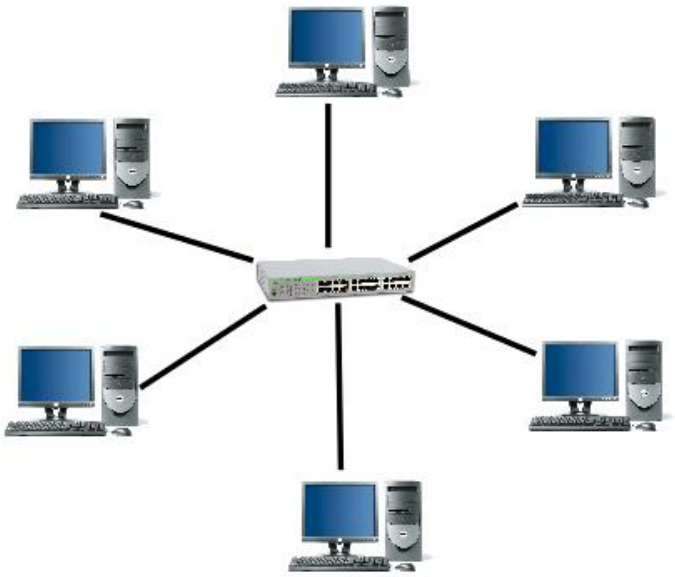


Figura 5. Topología en Estrella, las computadoras se conectan a un dispositivo central. Adaptado. Universidad Autonoma de México (sf). Administración de Redes http://redyseguridad.fi-p.unam.mx/proyectos/asmonredes/PHP/capitulo1.html

En este tipo de red es necesaria una computadora central muy poderosa rodeada de máquinas menos potentes que sirven únicamente como terminales de entrada y salida de datos.

Tabla 4.

Topología en Estrella, ventajas y desventajas.	
VENTAJAS	**DESVENTAJAS**
Estructura simple	Limitación en rendimiento y confiabilidad
Cada computadora es independiente de los demás	Su funcionamiento depende del servidor central
Facilidad para detectar computadoras que causen problemas en la red	Su crecimiento depende de la capacidad del servidor central
Fácil conexión	La distancia entre las estaciones de trabajo y el servidor
Permite añadir nuevas computadoras a la red	
Control de tráfico centralizado	
La falta de una computadora no afecta a la red	

Fuente: Adaptado de Gil P., Pomares J. y Candelas, J. (2010)

2.5.1.3. Topología en anillo.

Gil et al. (2010), la topologia en anillo conecta a las computadoras con un solo cable en forma de círculo, los extremos no están conectadas con un terminal.

Las señales pasan en una dirección y pasan por todas las computadoras de la red. Las computadoras en esta topología funcionan como repeaters, para mejorar la señal. Se trata de una arquitectura muy sólida, que pocas veces entra en conflictos con usuarios.

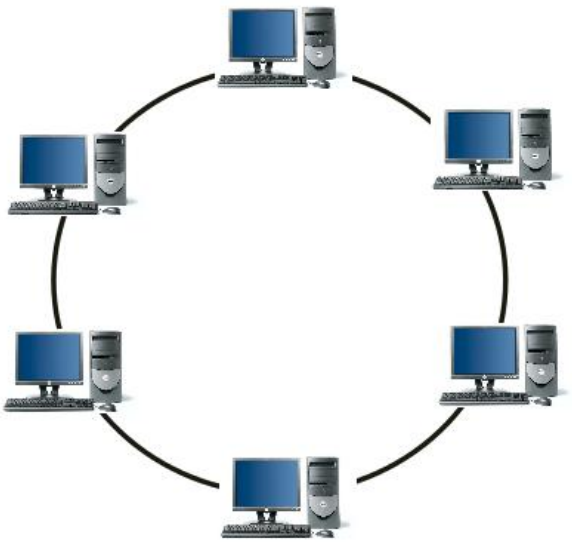


Figura 6. Las computadoras se conectan a un solo cable en forma de círculo. Adaptado: Universidad Autonoma de México (sf). Administración de Redes http://redyseguridad.fi-p.unam.mx/proyectos/asmonredes/PHP/capitulo1.html

Doble anillo (Token ring): Un método de transmisión de datos alrededor del anillo se denomina token passing. Las redes Token Ring no tienen colisiones.

Las redes Token Ring usan un sistema de prioridad sofisticado que permite que determinadas estaciones de alta prioridad designadas por el usuario usen la red con mayor frecuencia. Las tramas Token Ring tienen dos campos que controlan la prioridad: el campo de prioridad y el campo de reserva.

Tabla 5.

Topología en Anillo.

VENTAJAS	DESVENTAJAS
El sistema provee un acceso equitativo para todas las computadoras	La falla de una computadora altera el funcionamiento de toda la red.
El rendimiento no decae cuando muchos usuarios utilizan la red.	Las distorsiones afectan a toda la red.

Fuente: Adaptado de Gil P., Pomares J. y Candelas, J. (2010)

2.5.1.4. Topología en malla.

De acuerdo a Gil et al. (2010), esta topología principalmente nos ofrece redundancia. En esta topología todas las computadoras están interconectadas entre sí por medio de un tramado de cables.

Esta configuración provee redundancia porque si un cable falla hay otros que permiten mantener la comunicación. Muchas veces la topología en MALLA se va a unir a otra topología para formar una topología híbrida.

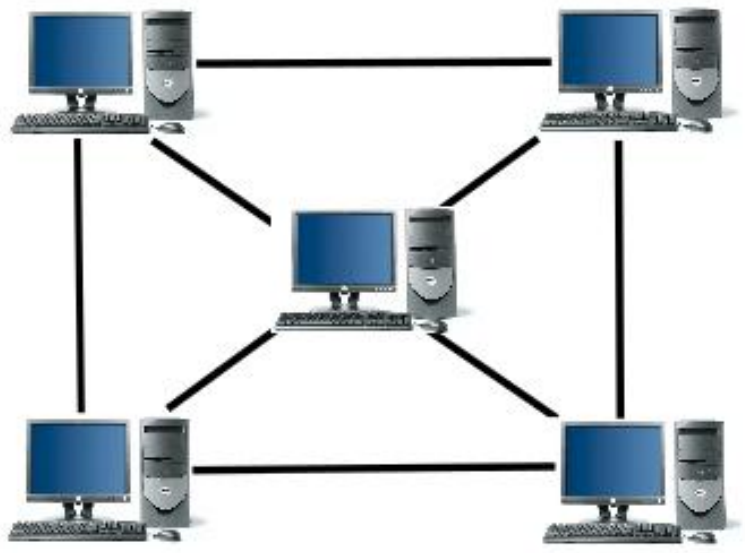


Figura 7. Las computadoras se conectan entre sí por medio de un tramado de cables. Adaptado. Universidad Autonoma de México (sf). Administración de Redes http://redyseguridad.fi-p.unam.mx/proyectos/asmonredes/PHP/capitulo1.html

Las redes en malla son aquellas en las cuales todos los nodos están conectados de forma que no existe una preeminencia de un nodo sobre otros, en cuanto a la concentración del tráfico de comunicaciones.

2.5.1.5. Topología en árbol.

Para Gil et al. (2010), esta topología combina características de la topología de estrella con la BUS. Consiste en un conjunto de subredes en estrella conectadas a un BUS. Esta topología facilita el crecimiento de la red.

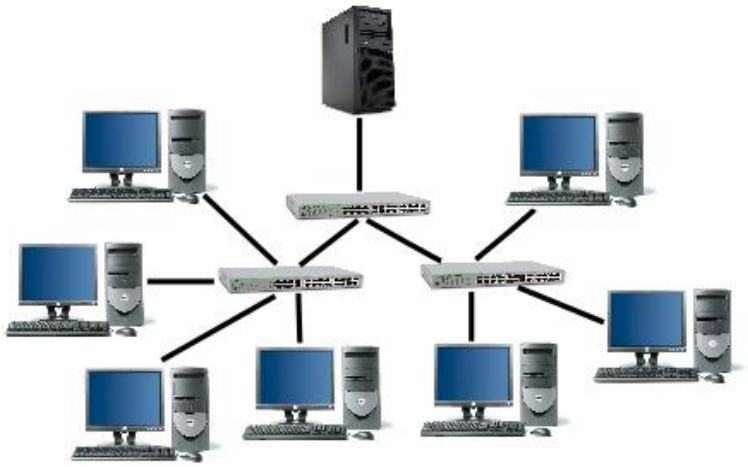


Figura 8. Combina las características de la topología de estrella con la de Bus. Adaptado Universidad Autonoma de México (sf). Administración de Redes http://redyseguridad.fi-p.unam.mx/proyectos/asmonredes/PHP/capitulo1.html

Tabla 6.

Topología en Red, ventajas y desventajas	
VENTAJAS	**DESVENTAJAS**
Cableado punto a punto para segmentos individuales	La medida de cada segmento viene determinada por el tipo de cable utilizado
Soportado por multitud de software y de hardware	Si se viene abajo el segmento principal todo el segmento se viene abajo con él
	Es más difícil su configuración
	Las redes de ordenadores se montan con una serie de componentes de uso común y que es mayor o menor medida aparece siempre en cualquier instalación

Fuente: Adaptado de Gil P., Pomares J. y Candelas, J. (2010)

2.5.2. Conexiones externas.

Además de los clientes y servidores de la red, es común la comunicación de datos entre la red de área local y el exterior, ya sea con usuarios de la misma o de distinta organización,

pertenecientes o no a la misma red corporativa, por ejemplo, una red corporativa puede estar constituida por distintas LAN en lugares geográficos distintos.

También es posible la comunicación entre dos LAN pertenecientes a distintas organizaciones. Esta comunicación se realiza a través de redes WAN. El acceso de un usuario remoto puede ser similar al acceso de un usuario local, disponiendo de los mismos servicios, aunque con rendimientos menores, debido a la inferior capacidad de transferencia de las líneas de transmisión de las redes WAN utilizadas en la conexión.

Para poder acceder a estos servicios remotos, en Gil et al., (2010) es necesario que las LAN posean nodos especializados en servicios de comunicaciones remotas, que también deben estar correctamente configurados. Las conexiones con el exterior requieren dispositivos especializados que dependen del tipo de conexión y de la WAN que se utilice. Por ejemplo, servidores y clientes RAS o de redes privadas virtuales, interfaces X.25, RDSI, ATM, etc.

2.5.3. Configuración de la red.

De acuerdo a Aguirre, X. (2011), la correcta configuración de las redes informáticas garantiza la estabilidad y robustez de la redes, evitará problemas futuros y además contribuye al ahorro económico de la empresa.

Se trabaja en la configuración de las Tarjetas de Red de los diferentes ordenadores. Se configuran la conexión a la red local, los correos electrónicos y se trabaja con perfiles, cualquier usuario puede trabajar en cualquier ordenador de la red. También se realiza la configuración de los diferentes periféricos de uso general: impresoras, scanner, el fax, etc.

En otro punto se trabaja la configuración del servidor o servidores: Sistema Operativo de red, Dirección IP, Máscara de Subred, Puerta de Enlace e Internet. Aquí cobra importancia la correcta configuración del BackUp para evitar pérdidas de datos involuntarias o mal intencionadas. En la actualidad se prefiere incorporar a sus redes informáticas un sistema de seguridad perimetral.

2.5.4. Correo electrónico.

Los archivos adjuntos de los mensajes de correo electrónico que reciba pueden contener virus del tipo gusano. Al abrir los datos adjuntos, este virus se activa y envía copias del mensaje y archivos adjuntos a todos los correos de la libreta de direcciones, replicándose a través del internet.

Para evitar este problema es necesario que se tome conciencia de no abrir correos con datos adjuntos provenientes de fuentes desconocidas.

2.5.5. Control de virus.

En la Revista Digital Ingenierias Aplicadas ITSC (2011) se define a los virus como programas maliciosos (malware) que infectan a otros archivos del sistema con el objetivo de modificarlos o dañarlos. La infección se produce al incrustar su código malicioso en el interior del archivo (normalmente un ejecutable) de esta forma dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

Se los conoce como virus por su similitud con los virus biológicos que afectan a los humanos, por su capacidad de propagarse, aquí los antivirus serían las medicinas que los controlan. Los virus informáticos tienen, básicamente, la función de propagarse a través de un software.

¿Cómo funcionan?:

- Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario; el código del virus se aloja en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.
- El virus toma el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables (.exe, .com, .scr, etc) que sean llamados para su ejecución, finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Vías de infección:

- Redes Sociales.
- Sitios webs fraudulentos.
- Redes P2P (descargas con regalo).
- Dispositivos USB/CDs/DVDs infectados.
- Sitios webs legítimos pero infectados.
- Adjuntos en Correos no solicitados (Spam)

En el documento Ciclo de vida de un virus de la Universidad Autonóma de Yucatan (2011) se indica que: “*Cuando se detecta y se aísla un virus, se envía al International Security Association en Washington D.C, para ser documentado y distribuido a los encargados de*

desarrollar los productos antivirus. El descubrimiento, normalmente ocurre por lo menos un año antes de que el virus se convierta en una amenaza para la comunidad informática.

En este punto, quienes desarrollan los productos antivirus, modifican su programa para que éste pueda detectar los nuevos virus. Esto puede tomar de un día a seis meses, dependiendo de quién lo desarrolle y el tipo de virus."

Si suficiente cantidad de usuarios instalan una protección antivirus actualizada, puede erradicarse cualquier virus. Hasta ahora, ningún virus ha desaparecido completamente, pero algunos han dejado de ser una amenaza.

Los virus y demás códigos maliciosos se dividen en varios tipos según los formatos en los que se ocultan y las rutinas que utilizan para infectar.

2.5.6. Muros de fuego (FireWall).

Firewall es un sistema o conjunto de ellos ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es como por ejemplo Internet, consiste en distintos dispositivos, tendientes a los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

El muro cortafuegos, sólo sirve de defensa perimetral de las redes, no defiende de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red, Stallings, W. (2004).

Routers y Bridges

Cuando se desea establecer comunicaciones externas entre redes LAN y WAN se necesita que los dos tipos de redes hablen el mismo idioma, para ello se utilizan los routers que son dispositivos que permiten convertir los protocolos que utilizan las redes LAN en protocolos

que utilizan las redes WAN y viceversa. Los Bridges son puentes que operan a nivel de enlace que se utilizan para conectar dos redes LAN.

Con los adelantos tecnológicos estos dispositivos se han convertido en computadoras especializadas que le permiten detectar, el camino más corto y más descongestionado hacia el Router de la red destino. Los routers están configurados de tal forma que están en capacidad de "tomar decisiones" en base a filtros, reglas y excepciones.

Tipos de Firewall

- Filtrado de Paquetes
- Proxy-Gateways de Aplicaciones
- Dual-Homed Host
- Screened Host
- Screened Subnet
- Inspección de Paquetes

Firewalls Personales

Según Stallings, W. (2004), estos Firewalls son aplicaciones que permiten conectarse a una red insegura sin comprometer la integridad de la computadora del usuario, manteniéndola a salvo, evitando inconvenientes como infección de virus y la pérdida de la información almacenada.

Políticas de Diseño de Firewalls.

Stallings, W. (2004), indica que las políticas de accesos en un Firewalls se diseñan basadas en sus limitaciones, capacidades, vulnerabilidades y amenazas que se puede presentar en una red externa insegura

El primer paso para instaurar normas de seguridad es determinar qué puntos vamos a proteger, que usuarios deben acceder y a qué recursos del sistema. Las políticas de seguridad deben responder las siguientes preguntas:

- ¿Qué se debe proteger? Se protegerán todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse? De cualquier intento de acceso no autorizado y contra ataques desde el interior.

- ¿Cómo protegerse? La forma en que se establecerá el nivel de monitorización, control y respuesta.

Se debe aplicar alguno de los siguientes paradigmas o estrategias:

Paradigmas de seguridad

- Se permite cualquier servicio excepto aquellos expresamente prohibidos.
- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos.

Estrategias de seguridad

- Paranoica: se controla todo, no se permite nada.
- Prudente: se controla y se conoce todo lo que sucede.
- Permisiva: se controla pero se permite demasiado.
- Promiscua: no se controla (o se hace poco) y se permite todo.

Restricciones en el Firewall

La tarea fundamental que realizan los Firewalls, es permitir o denegar servicios, de acuerdo al tipo de usuario y de su ubicación.

Permiso de salida para servicios restringidos: Cuando los usuarios provengan de la red interna, podrán acceder a servicios externos predefinidos por el administrador.

Para Stallings, W. (2004), usuarios externos con permiso de entrada desde el exterior: usuarios externos que acceden a la red interna para realizar consultas o para prestar servicios a la misma, en este caso se debe tener mucho cuidado al otorgar permisos ya que es la parte más propensa a producir vulnerabilidades, en tal caso las cuentas deben ser activadas y desactivadas de acuerdo a la necesidad.

Beneficios de un Firewall

Como se indica en Castro, M., Díaz, G., Alzórriz, I. & Sancristóbal, E. (2014); El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos. El uso de Firewalls es imprescindible debido a la disminución del número disponible de direcciones IP, para solucionar este problema el Firewall permite utilizar un traductor de

direcciones con la finalidad de que las intranets puedan adoptar direcciones sin clase para salir a Internet.

Los Firewalls también permiten llevar estadísticas del ancho de banda consumido por el tráfico de la red, y los procesos más influentes en el tráfico, facilitando al administrador de la red restringir el uso de estos procesos y economizar el ancho de banda disponible.

Limitaciones de un Firewall

Castro, M. et al. (2014), indica que la limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall “no es contra humanos” es decir que si un intruso logra entrar a la organización y descubrir claves de acceso o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él no protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna.

2.5.7. Control de ataques a la red.

De acuerdo a Stallings, W. (2004); existen dos tipos de ataques informáticos: ataques activos, que producen cambios en la información y en los recursos del sistema, y ataques pasivos que registran el uso de los recursos y/o acceden a la información almacenada o transmitida.

Tipos de ataques contra redes y sistemas informáticos

- Actividades de reconocimiento de sistemas

- Detección de vulnerabilidades en los sistemas
- Robo de información mediante la interceptación de mensajes
- Modificación del contenido y secuencia de los mensajes transmitidos
- Análisis de tráfico
- Ataques de suplantación de identidad (IP Spoofing, DNS Spoofing, SMTP Spoofing, snooping).
- Modificaciones del tráfico y tablas de enrutamiento.
- Conexión no autorizada a equipos y servidores
- Introducción de código malicioso (malware)
- Ataques de Cross-Site Scripting XSS
- Ataques de inyección de código SQL
- Ataques contra los sistemas criptográficos.
- Fraudes engaños y extorsiones.
- Ataques DoS o Denial of Services.
- Ataques de denegación de servicios distribuidos DDoS.

La organización debe contar con las políticas y herramientas que permitan eliminar o minimizar los efectos en el sistema informático, por la acción de este tipo de ataques.

2.6. Seguridad de las Aplicaciones.

Evaluar la seguridad de las aplicaciones que está utilizando la empresa, los datos de entrada, los datos de salida, la integridad de las bases de datos y la documentación de las aplicaciones.

2.6.1. Software.

Sistemas operativos:

Se debe verificar que los Sistemas Operativos estén actualizados con las últimas versiones y parches de seguridad; si se instalaron correctamente y si los instaladores del SO se encuentran en un lugar seguro. Determinar las causas por las que se ha omitido estos procedimientos.

Software básico:

El auditor debe conocer los productos de software básico que han sido adquiridos y para que usuarios. Debe contar con un inventario en el que conste: nombre del producto, versión, fecha de compra, fecha de la última actualización, usuarios, etc.

En lo relacionado con el software desarrollado en la empresa, el auditor debe verificar que éste cumpla con las necesidades de la organización, no disminuya las prestaciones del Sistema, esté de acuerdo a las políticas de la empresa y que se encuentre debidamente documentado.

Software de teleproceso (Tiempo Real).

No se incluye en Software Básico. Las consideraciones anteriores son válidas para éste también.

Tunning.

Según Coronel, C., Steven, M. y Rob, P. (2011) se conoce como tunnig a las técnicas de observación, que permiten evaluar el comportamiento de los Sistemas. Para realizar el tunning se debe establecer planes y programas de acción.

Optimización de los sistemas y subsistemas.

Los responsables del área técnica deben realizar acciones permanentes de optimización como resultado de la aplicación de los tunnings. El auditor verificará que las acciones fueron efectivas y no comprometieron a los sistemas.

2.6.2. Bases de Datos.

Para, Coronel, C., et al. (2011) el diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunos problemas derivados de la escasa experiencia que se tiene sobre la problemática general de los usuarios de Bases de Datos.

2.6.3. Aplicaciones en PCs.

Gómez, A. (2011), debido a que los usuarios no poseen conocimientos suficientes de informática, a la escasa o poca capacitación sobre las técnicas para vulnerar los sistemas y a que las computadoras debido a la cantidad de tareas que ejecutan presentan problemas para establecer una configuración segura; es fácil que los usuarios sean engañados por técnicas de ingeniería social.

Para evitar estos problemas de seguridad hay que establecerse una serie de normas para la configuración y uso de los computadores:

- Utilizar procesos de autenticación de usuarios utilizando protocolos seguros.
- Utilizar un corta fuegos para filtrar las conexiones a internet.
- Actualizar periódicamente el sistema a través de servicios confiables.
- Utilizar un antivirus que se actualice constantemente.
- Aplicar la seguridad de sistemas de ficheros.
- Desactivar todos los servicios y cerrar puertos que no sean necesarios.
- Limitar la compartición de discos, carpetas e impresoras.
- Crear una estructura adecuada de cuentas y grupos de usuarios, limitar privilegios y permisos de usuarios.
- Trabajar en forma segura con el equipo, no abrir correos electrónicos sospechosos, ni ficheros adjuntos inesperados, no ejecutar programas poco fiables, eliminar los datos y carpetas temporales, cookies; etc.
- Documentar todos los cambios realizados en el sistema.
- Realizar copias de seguridad periódicas del sistema.
- No utilizar operaciones de riesgos para el sistema: descarga de ficheros desde servidores FTP y servidores Web poco confiables; utilización de aplicaciones de intercambio de ficheros, instalación de salvapantallas, etc.

Es responsabilidad del departamento técnico fijar que aplicaciones a más de las necesarias para el funcionamiento de la organización se debe instalar en las Pcs de cada usuario, así como deshabilitar el acceso a descargas de música, vídeo, pornografía, redes sociales y cualquier otra página Web que no tenga relación directa con el trabajo. Se deberá advertir a los usuarios sobre las sanciones que acarrea el incumplimiento de las normas de seguridad.

2.6.4. Ciclo de Vida.

El desarrollo de sistemas es un término que nació del Análisis y Programación de Sistemas y Aplicaciones; una Aplicación recorre las siguientes fases:

- Pre requisitos
- Análisis
- Diseño
- Programación
- Pruebas
- Explotación.

Todas las fases anteriores requieren de control interno, para evitar el aumento en los costes y que el sistema no cumpla con las necesidades del cliente. Además se debe comprobar que los programas hagan exactamente lo que se espera de ellos y garanticen la seguridad de la información.

Una auditoría de Aplicaciones pasa necesariamente por la observación y el análisis de cuatro consideraciones:

- Revisión de las metodologías utilizadas
- Control Interno de las Aplicaciones
- Estudio de Vialidad de la Aplicación
- Definición Lógica de la Aplicación
- Desarrollo Técnico de la Aplicación
- Diseño de Programas
- Métodos de Pruebas
- Documentación
- Equipo de Programación
- Satisfacción de usuarios
- Control de Procesos y Ejecuciones de Programas Críticos.

2.7. Evaluación de la administración centro de procesamiento de datos (CPD).

Evaluar la organización y administración del departamento de sistemas, asignación de tareas, procedimientos y responsabilidades del personal, con el objetivo de brindar un ambiente adecuado y seguro para brindar un servicio de calidad a la institución.

Piattini, M. (2008), el Centro de Procesamiento de Datos (CPD) o Centro de cómputo, es el conjunto de recursos físicos, lógicos, y humanos que operan los equipos informáticos.

Las principales funciones que se requieren para operar un centro de cómputo son las siguientes:

- Operar y mantener disponible el sistema de computación.
- Ejecutar los procesos asignados conforme a los programas.
- Revisar los resultados de los procesos e incorporar acciones correctivas
- Realizar las copias de respaldo (back-up)

- Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
- Realizar labores de mantenimiento y limpieza de los equipos del centro de cómputo.
- Aplicar en forma estricta las normas de seguridad y control establecidas.
- Cumplir con las normas, reglamentos y procedimientos establecidos por la Dirección para el desarrollo de las funciones asignadas.

2.7.1. Administración del CPD.

Para Hernández, R. (2003), en este aparatado se debería analizar y observar básicamente lo siguiente:

- Responsabilidades puntuales a cada empleado del CPD y la respectiva documentación.
- Planes formales del CPD tanto a corto como a largo plazo
- Determinar el grado de conciencia de los empleados en cuanto a la seguridad de la información.
- Forma en que los usuarios solicitan asesoramiento o servicios al CPD.
- Mantenimiento preventivo en el CPD.
- Inventario de los sistemas de información y sus características:
  Nombre
  Lenguaje
  Departamento de la empresa que genera la información.
  Departamentos de la empresa que usan la información.
  Equipamiento para el funcionamiento del sistema.
  Fechas en que la información es necesitada con urgencia.
  Importancia estratégica que tiene la información del sistema para la empresa.
  Inventario detallado de los equipos donde incluya:
  Hardware: dispositivos instalados en cada máquina, número de serie, datos sobre procesadores, tarjetas, teclados, terminales, PCs, impresoras, unidades de disco, cableado de la red, servidores, routers, etc.
  Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, número de licencias, etc.
  Principales archivos que contienen los equipos.
  Configuración de los equipos.
  Ubicación de los equipos.
  Nivel de uso de los equipos.

- Procedimiento para hacer conocer las normas, directivas o modificaciones.
- Quién realiza las operaciones en las PCs: de mantenimiento, instalación de virus, copias de respaldo, desfragmentar discos, modificar passwords, entre otras.

2.7.2. Capacitación.

Una vez capacitado el empleado en la realización de sus tareas diarias y conozca claramente el manejo de (los) sistema(s) que va a utilizar en su trabajo, se debe comunicar las políticas de seguridad de la información y los procedimientos establecidos en la empresa, así mismo se debe entregar una copia impresa de las medidas básicas y hacerle firmar un documento en el que acepta conocer las normas impuestas por la empresa y las consecuencias que acarrea su incumplimiento, este documento debe ser archivado junto con la carpeta del empleado.

2.7.3. Backups.

Las copias de seguridad según Gómez, A. (2011), son el principal método de recuperación y no tener un manual de procedimientos para la realización de backups puede provocar graves problemas a la organización.

Es necesario que exista un procedimiento establecido por escrito para la realización de backups, el mismo que debe contener como mínimo:

- Tipo de backup
- Medios de almacenamiento
- Lugar donde se guardan estos medios.
- Frecuencia de realización de los backups
- Herramientas a utilizar.
- Personal encargado del proceso.
- Documentación de los backups:
- Datos que contiene
- Fecha de realización
- Fecha de restauración
- Errores presentados

2.7.4. Documentación.

De acuerdo a Gómez, A. (2011), si no existe un buena documentación, la información puede ser incorrecta, inconsistente y desactualizada dificultando la administración de incidentes. La documentación debería contener:

- Diagrama de las instalaciones, identificación de PCs, equipos y puestos de trabajo.
- Número de serie del hardware
- Número de licencia del software
- Inventarios de hardware y software
- Falla en equipos y acciones de mantenimiento
- Configuración de equipos y servidores
- Cambios en la topología de la red
- Personal externo autorizado
- Planes de seguridad, procedimientos formales, documentos y manuales de soporte para la gestión de la seguridad de la información. La documentación debería contener los siguientes datos:
    - Plan de contingencia
    - Política de seguridad
    - Manual de procedimientos
    - Manual del usuario (hardware y software)
    - Manual de seguridad para el sistema
    - Manual de seguridad para el usuario

Los siguientes documentos deben realizarse para la documentación del desarrollo de sistemas:

- Objetivos
- Alcances
- Diagrama general, de funciones, de procesos
- Diagrama de flujo
- Archivos de entrada salida
- Registro de modificaciones
- Lenguaje de programación
- Sectores de la empresa a los que afecta
- Descripción del hardware y software utilizados
- Características de seguridad

2.8. Evaluación del plan de seguridad informática.

Evaluar el plan de seguridad de la empresa con la finalidad de detectar debilidades y los posibles efectos en la seguridad, para de esta forma desarrollar sugerencias que permitan minimizar estos efectos y garantizar la continuidad del servicio.

Piattini, M. (2008); en la auditoría es necesario revisar si existe este plan, si es completo y actualizado, o si existen planes diferentes de acuerdo a los entornos, evaluar su idoneidad, y si el mismo permite la reanudación de operaciones en el tiempo mínimo que evite pérdidas económicas a la organización.

2.8.1. Administración de incidentes.

Canales, G. y Marroquín, K. (2012); se debe analizar el procedimiento actual para la administración de las secuelas de un incidente. El procedimiento debe documentar cómo hacer frente a los diferentes errores que pueden devastar la infraestructura de TI (Tales como la pérdida completa de los servidores, los datos, routers, puentes, comunicación, enlaces, etc.)

Al buscar la manera de hacer frente a estas pérdidas, se dará cuenta de que hay soluciones alternativas. Antes de determinar y documentar un proceso de recuperación de desastres, debe rediseñarse las configuraciones que no tienen redundancia.

También debe crear una lista de comprobación para verificar si todo ha sido restaurado a su estado normal.

Al final, el plan debe ser completo, integral y actual. Por Completo, se refiere a que debe ser lo suficientemente detallada para incluir cada etapa de recuperación.

En momentos de estrés, y cuando las personas encargadas no están presentes, debe servir como un paso a paso de cómo hacerlo. Debe ser integral e incluir todos los elementos dentro del centro de datos y por fuera, todos los componentes críticos, y todas las unidades de negocio.

2.8.2. Backup de equipos.

En Piattini, M. (2008); un elemento fundamental dentro del Plan de Seguridad es la existencia de un centro de respaldo, con el equipamiento de hardware y software; dependiendo de la capacidad de la empresa existen diversas alternativas a la hora de implantar un centro alternativo.

- Si no se dispone de un Centro Alternativo y no existen copias de seguridad externas, es posible que nunca se lleguen a recuperar los datos, programas y la documentación del sistema afectado.
- Transporte periódico de copias de seguridad a un almacén, existe un intento de plan de recuperación del negocio, sin embargo el tiempo de recuperación puede ser alto.
- Centro Alternativo Frío, cuenta con un equipamiento suficiente de hardware, software y comunicaciones para mantener los servicios críticos de la organización.
- Centro Alternativo Caliente, cuenta con un equipamiento de hardware, software y comunicaciones necesario para mantener los servicios críticos de la organización, y en el que además los equipos se encuentran en funcionamiento y disponen de una réplica de todos los datos y aplicaciones del sistema informático, así el tiempo de recuperación es de pocas horas.
- Centro Alternativo Caliente en configuración en espejo (mirror), se trata de un Centro Alternativo con el mismo equipamiento que el Centro Principal y que trabaja de un modo paralelo a este, el tiempo de recuperación es casi inmediato, Gómez, A. (2011).

2.8.3. Recuperación de desastres.

Canales, G. & Marroquín, K. (2012); el Plan de Recuperación de desastres debe especificar objetivos y prioridades, para esto es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan el funcionamiento del sistema informático, recuperar los datos, aplicaciones y servicios básicos que son el soporte al negocio de la organización:

- Disponibilidad de un Centro Alternativo o Centro de Reserva para la ubicación de los principales recursos informáticos (servidores y bases de datos)
- Existencia de líneas de back-up para las comunicaciones
- Sistemas de almacenamiento RAID en los servidores
- Implantación de clusters de servidores con balanceo de carga
- Herramientas para llevar a cabo una replicación de los documentos y las bases de datos, que puede ser síncrona, asíncrona o periódica
- Composición del equipo que coordinara las fases de recuperación

Un procedimiento para la recuperación frente a desastres debería contemplar las siguientes actividades:

Detección y respuesta al desastre en el Centro Principal:

- Adopción de medidas de contención previstas dependiendo del tipo de desastre: incendio, inundación, explosión.
- Comunicación a las personas y organismos externos indicados según el tipo de desastre.
- Traslado de la actividad al Centro Alternativo:
- Traslado del personal necesario al Centro Alternativo
- Puesta en marcha de los servicios y equipos informáticos
- Volcado de los datos disponibles en las copias de seguridad más recientes
- Recuperación de las aplicaciones y servicios necesarios para la continuidad de las operaciones, priorizando el orden de esta recuperación en función de su importancia o criticidad para el funcionamiento de la organización.
- Verificación del nivel de servicio recuperado
- Recuperación del Centro Principal siniestrado.

CAPÍTULO III.
DESARROLLO DE LA AUDITORIA.

Luego de la visita preliminar para conocer la empresa y los responsables del CPD, se procedió a elaborar las preguntas agrupándolas por componentes: Seguridad Física, Seguridad Lógica, Seguridad de la Red, Seguridad de las Aplicaciones, Administración CPD, Plan de Seguridad; (Anexos 2-7).

En este capítulo se detalla la información recopilada mediante las encuestas realizadas a los responsables del CPD de acuerdo a los componentes de la auditoría establecidos; información que nos servirá posteriormente para realizar el análisis y determinar las debilidades, efectos y recomendaciones que permitan eliminar o por lo menos minimizar los impactos de estas debilidades.

3.1. Seguridad Física

3.1.1. Equipamiento.

Tabla 7.

Servidores instalados CPD Edpacif.				
Servidor	**Procesador**	**Memoria**	**Discos Duros**	**Tecnología**
IBM Proliant	ML350 G6 QUAD CORE, con fuente de redundancia	4 Gigas de RAM	3 discos duros de 164 MB	SAS (RAID5)
HP Proliant	DL380 G5 QUAD CORE, con fuente de redundancia	4 Gigas en RAM	3 discos duros de 72 Gb	(RAID5)
HP Proliant ML350 G4	Procesador INTEL XEON	3 discos duros de 164 MB	4 Gigas en RAM	SAS RAID

Fuente: Administrador CPD Edpacif.

Tabla 8.

Características de las PC´s			
Cantidad	**Procesador**	**Ram**	**Disco**
60	CORE I3	2GB	80GB

Fuente: Administrador CPD Edpacif.

Sin CD ROM, ni multi reader, las últimas máquinas adquiridas son con procesador CORE i3. Solo se permite el uso de tres laptops en la empresa: Jefe de Sistemas, Gerente y Auditora Interna.

3.1.2. Control de acceso físico al CPD.

En la instalación del CPD no se hizo un análisis costo beneficio para determinar los controles de acceso físico necesarios, porque cuando la empresa inicio no contaba con un área específica para sistemas, actualmente ya se cuenta con el área destinada a sistemas y se implementó el control de acceso basado en la experiencia del administrador, el acceso al

área de servidores es solo para el personal de sistemas; no existió asesoramiento de terceros para establecer los controles de acceso, se lo realizó en base a la experiencia en trabajos anteriores del encargado del CPD.

Se restringe el acceso al CPD a las personas que no pertenecen al mismo, utilizando los siguientes controles:

- Tarjetas de entrada, en la garita de ingreso y áreas de la planta.
- Guardias de seguridad, en la garita de entrada.
- Circuito cerrado de televisión, en todas las áreas productivas y para control de los exteriores de la empresa, están ubicadas en puntos estratégicos: puerta de entrada, pasillos, etc.

En la visita a la empresa se pudo comprobar que no existe ninguna cámara dirigida hacia la entrada del CPD.

Para el ingreso del personal que necesite entrar al CPD se les permite el ingreso solo si trae la tarjeta de proximidad, si la persona no la trae, tiene que ir a recursos humanos para que le entreguen una, caso contrario no puede trabajar ya que tiene que timbrar en los relojes internos de planta, con la misma tarjeta puede utilizar el comedor si tiene el permiso correspondiente.

En el caso de personas ajenas a la empresa el guardia de la entrada anuncia su presencia al empleado solicitado, una vez aceptado el ingreso un guardia le entrega una credencial de visita y acompaña al visitante hasta la oficina donde es recibido por el empleado; al finalizar la visita el empleado acompaña al visitante hasta la garita de guardias.

3.1.3. Control de acceso a los equipos.

El acceso a los equipos se controla mediante una clave habilitada en la BIOS, casi todas las máquinas no cuentan con CD’s, ni lectoras de memoria y en las que los tienes estos están deshabilitados, nunca hubo robo de información por medio de estos dispositivos. En la empresa nunca se pide CD ROM ni lectores de tarjetas.

Existen programas que bloquean la entrada de dispositivos USB, en la empresa nunca se pide CD’s ni lectores de tarjetas, únicamente sistemas y subgerencia tiene acceso a ellos ya que son los únicos que cuentan con estos dispositivos. Quién necesite sacar información de

CD's y memorias tiene que ir obligatoriamente a Sistemas para analizar los medios en busca de información dañina y virus, luego se procede a copiar la información que necesitan en sus máquinas vía internet.

Los dispositivos extraíbles se guardan en gabinetes con llave en un lugar apropiado fuera del alcance del personal y con las medidas de seguridad que garanticen su correcto funcionamiento, las llaves de los gabinetes las tiene el administrador bajo su custodia. El técnico de sistemas realiza el control de los dispositivos que se instalan en las PC's de acuerdo al cronograma previamente establecido, aproximadamente cada tres meses.

Los servidores de la empresa permanecen prendidos las 24 horas del día de lunes a domingo.

3.1.4. Dispositivos de Soporte.

El administrador del CPD indica que la empresa cuenta con los siguientes dispositivos de soporte para el equipamiento informático:

Tabla 9.

Equipamiento CPD Edpacif	
Equipo	**Descripción**
Aire acondicionado	El CPD cuenta con aire acondicionado, temperatura entre los 18º y 20º que es lo recomendado por lo proveedores de equipos.
Extintores de incendios	Son equipos manuales de polvo químico, se encuentran ubicados en los exteriores de las áreas, su cantidad y ubicación lo determinó Seguridad Industrial
UPS	Hay 4 unidades de poder ininterrumpido de 6 Kva cada una, banco de baterías de una hora de duración, funcionan todo el tiempo.
Otros	Cuenta con equipos que evitan la sobrecarga de la red eléctrica, así como hardware especial de aislamiento y protección de dispositivos magnéticos

Fuente: Muñoz, A. (2014).

3.1.5. Edificio.

Como se mencionó anteriormente (3.1.2. Control de acceso físico) cuando inicio la empresa no se contaba con un área específica para el área de sistemas por lo que al diseñar el edificio no se tomo en cuenta la seguridad de los datos y de los equipos. El área donde se

encuentra el CPD está ubicado en un local lo suficientemente grande previendo el crecimiento futuro de la red, cuenta con techo falso y pisos de fácil acceso para pasar el cableado, elaborados con materiales impermeables e incombustibles al igual que las paredes.

Está ubicado en la planta baja, cerca del backbone para facilitar las conexiones, el personal que labora en el CPD está capacitado para actuar en caso de incendio, no se permite comer ni tomar bebidas, se deben seguir ciertos procedimientos estandarizados para la recepción y almacenaje de papel, se mantiene en un lugar de fácil acceso y es conocido por todos los números telefónicos del cuerpo de bomberos de la localidad. Cuenta con planos de las canalizaciones de agua, luz y sanitaria, las mismas que no interfieran con la red, el CPD se encuentra alejado de áreas donde se utiliza o almacena materiales inflamables, tóxicos o corrosivos, el mobiliario del CPD está fabricado con materiales no combustibles.

Las ventas no cuentan con protecciones, el área de trabajo del personal del CPD es un poco reducida, constatándose que falta espacio para colocar los equipos en reparación, los mismos que permanecen en el suelo junto a la ventana.

3.1.6. Cableado.

El administrador del CPD indica que en la instalación del cableado se consideró la ubicación de los canales, para que no sean afectados por inundaciones, cortes eléctricos, desagües o campos magnéticos, para el cableado se utilizó la norma IEEE con cableado estructurado STP categoría 6; para evitar interferencias, tanto el cableado eléctrico como el de Red van entubados, y cuando van por la misma canaleta, esta tiene una división.

Los daños en los cables es responsabilidad del Departamento de Mantenimiento el mismo que prevé los daños cuando realiza trabajos en la planta.

Durante y después de alguna emergencia se controla el acceso al centro de cómputo.

3.2. Seguridad Lógica.

3.2.1. Identificación y autenticación.

Altas:

Los datos que se guardan en el perfil de usuario son: ID del usuario que tiene relación con código de recursos humanos

Password:

Apellidos y Nombres, Departamento o Unidad a la que pertenece, Fecha de expiración del password.

Bajas:

Recursos humanos informa las desvinculaciones y cambios de funciones del personal, existen procedimientos para la eliminación de claves, se llevan registros de las claves eliminadas, los mismos que se almacenan con la finalidad evitar repetir nombres de usuario y saber hasta qué fecha el usuario accedió al sistema.

Estos procedimientos se realizan inmediatamente después que el empleado se ha retirado de la empresa.

Gestión y Mantenimiento:

Cuentan con una política documentada para la gestión de claves de acceso, la administración de las claves es responsabilidad del personal de sistemas. Las claves de acceso deben estar conformadas por letras y números, mínimo 4 caracteres, máximo 8 caracteres, se deben cambiar o actualizar cada tres meses.

Para proteger las claves se utilizan técnicas de cifrado, para la asignación de claves se verifica que el usuario tenga la autorización del jefe inmediato del área donde trabaja el usuario. En caso de que el usuario cambie de función, se lleva un registro actualizado de los cambios de privilegios.

No se cuenta con un registro de los intentos de aceptación y rechazo de claves de usuario en el sistema, ni se lleva un registro que indique la hora, fecha y aplicación que utilizo el usuario; no se realizan seguimientos a los registros de accesos no autorizados o autorizados y fallidos, no existen registros de errores al ingresar datos, por cada aplicación; el tiempo de conexión no está limitado al horario de trabajo.

Cuando el usuario olvidó o reveló su clave se procede al cambio inmediato de la misma, al detectar que existen claves sin usar se procede con su des habilitación; si el usuario se encuentra en goce de sus vacaciones no se realiza ningún procedimiento. Estos procedimientos no son registrados.

Autenticación:

Al tipiar el password se muestran Asteriscos para evitar que el mismo sea revelado, los datos de autenticación se guardan encriptados utilizando algoritmos de criptografía, estos datos son clasificados como confidenciales. El acceso a estos datos es solo para el personal de sistemas, la autenticación es para toda la red y por aplicación.

No se bloquea el acceso luego de un número de intentos fallidos, el equipo espera un tiempo para mostrar nuevamente la ventana de ingreso de contraseña.

No se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos pero para mensajes externos si se las usa ya que para algunos documentos son necesarias.

Password:

El usuario genera su clave, la misma que debe contener letras y números, mínimo 4 caracteres y máximo 8 caracteres, no se permite que el password tenga el nombre de la empresa o el nombre del usuario, tampoco dos cuentas pueden tener el mismo password tanto para los usuarios como para el administrador, el password no puede ser el mismo que el ID de usuario.

El password debe ser cambiado cada tres meses, no está permitido cambiar el password en cualquier momento; si el usuario pierde o revela el password debe denunciar al departamento de sistemas. No se guardan los passwords utilizados por cada usuario, si se capacita a los usuarios sobre la administración de su password se les enseña a:

- No usar password fáciles de descifrar
- No divulgarlas
- No escribirlas o guardarlas en lugares fáciles de encontrar
- No usar la misma clave para varios servicios
- Comprender que el password es el principal método de seguridad

3.2.2. Roles.

Las claves se asignan por usuario, los permisos de (lectura, escritura, ejecución, eliminación, todos los anteriores) son asignados de acuerdo a las funciones del usuario. El Id hace referencia a una persona; los usuarios se clasifican en:

- Administradores Sistema, son funcionarios del área de sistemas que realizan operaciones de mantenimiento, actualización y monitoreo de los sistemas.
- Ejecutivos y Directivos, utilizan la información de los sistemas como base para la toma de decisiones.
- Directores áreas, toman la información para la realización del trabajo de su área, proponen nuevas utilidades del sistema.
- Operadores, ingresan información a los sistemas a través de los dispositivos conectados al computador (principalmente a través del lector de código de barras), es decir alimentan con datos el sistema.

3.2.3. Transacciones.

Se permite hacer ciertas transacciones a unos usuarios que otros no pueden hacer dependiendo del tipo de usuario y del Grupo. Se restringe el acceso a programas determinados a ciertos usuarios mediante la definición del perfil, evitando de esta manera acciones no autorizadas como la instalación de programas por parte de usuarios no autorizados.

3.2.4. Limitaciones a los servicios.

Si existe en la empresa productos de software cuya licencia limite su uso a un número determinado de usuarios. El administrador ha establecido limites al uso simultaneo de ciertas aplicaciones.

3.2.5. Modalidad de acceso.

Existe un procedimiento para la asignación de permisos de acceso, se asigna por usuario y aplicación. El administrador es quién otorga estos permisos y se lo hace por perfil y con autorización del jefe inmediato de cada área.

Este procedimiento se encuentra debidamente documentado.

3.2.6. Ubicación y Horario.

El tiempo de conexión limitado al horario de trabajo, no se restringe el acceso a determinadas horas del día o días de la semana para mayor control, no se consideran necesarias estas restricciones de acceso.

3.2.7. Control de acceso interno.

Los mecanismos de control de acceso que se utilizan son:

- Password y Listas de Control de acceso, las que se manejan por sistema integrado, con actualización manual semanalmente. Se usa encriptación para almacenarla.
- Interfaces de usuarios restringidas, solo ven lo que les está permitido, con la vista de menús.
- Encriptación, se encriptan los passwords y las cuentas de usuario.
- Protección de puertos.

3.2.8. Control de acceso externo.

Mecanismos de control de acceso externo:

- Gateways o firewalls seguros.
- Acceso de personal contratado, consultores y mantenimiento.
- Autenticación basada en host.
- No existe acceso externo a los datos, desde internet o desde módem.

Para mantener la integridad y confiabilidad de los datos, se tiene en cuenta:

- Alguna forma de identificación y autenticación.
- Control de acceso para limitar lo que se ve, lee, borra, modifica, etc.
- Firmas digitales.
- Copias de seguridad de información pública en otro lado, no en la misma máquina.
- Se prohíbe el acceso público a bases de datos vivas.
- Verifican que los programas y la información pública no tenga virus.
- Usan alguna forma de acceso remoto para cambiar la configuración del sistema.

3.2.9. Administración de personal.

Se tiene una máxima separación de funciones, se otorga el mínimo permiso de acceso requerido para cada puesto, se considera los requerimientos de experiencia y conocimiento para cada puesto.

La empresa no tiene establecido un procedimiento de capacitación continua para el personal. El personal es consciente de la importancia de la información como recurso valioso para la empresa.

3.3. Seguridad de la Red

3.3.1. Topología de Red.

Existe un gráfico topológico desactualizado Componentes de la red:

- 60 Pcs distribuidas en la empresa.
- 1 servidor de archivos.
- 1 servidor de Internet fibra óptica 1 servidor de internet satelital.

Descripción de la red:

- Enlaces radiales y satelitales
- Fibra óptica UTP en conexiones internas Switches

3.3.2. Conexiones Externas.

Al contar con un sistema integrado la empresa no necesita tener oficinas ni sucursales en otras ciudades, por lo que todos los procesos productivos y administrativos se centralizan en la planta de empacado ubicada en Pedernales.

Todos los procesos desde la recepción del productos se controlan en línea, ingresando los datos desde las Pcs de producción mediante el ingreso de códigos de barras, lo que permite en un momento dado rastrear una caja del producto desde su origen (camaronera) hasta el lugar de comercialización (en cualquier parte del mundo), este es el sistema de trazabilidad que la empresa ofrece a sus clientes.

Servidores de internet La empresa cuenta con un servidor de internet con fibra óptica y como respaldo y ante posibles caídas de la conexión ADSL se cuenta con una conexión satelital lo que permite a la empresa mantenerse en contacto con sus clientes a nivel mundial.

3.3.3. Configuración de la red.

Los datos van encriptados y pasan por el firewall, existen controles de acceso adecuados a los servidores conectados a internet, estos se encuentran en un cuarto de servidores con llave la misma que es custodiada por el administrador de sistemas.

No se comparte los discos de las PCs en la red; en el servidor de archivos se comparten carpetas, cada usuario tiene su carpeta con información referente a su puesto de trabajo, no se puede ver las carpetas de mails de los compañeros de trabajo, estas están protegidas por una contraseña que la pone el administrador.

En cuanto a la fiabilidad existen medios de transmisión de datos alternativo mediante la implementación de switchs extras, se realizan backups continuamente, si no funciona ADSL existe una redundancia de acceso a internet ya que se cuenta con dos servidores de internet, uno para la red con fibra óptica y otra conexión satelital.

A nivel de puertos se deshabilitaron todos los puertos no necesarios aplicando la política de solo se habilitan los puertos de red necesarios, además se hacen pruebas de los puertos a nivel de servidores, así como del firewall mediante software.

Se realizan pruebas periódicas de hackeo utilizando MTEXPLOIT y WARESHARK, además los puertos se prueban con un escaneador. Todos los días se hace chequeo de la red y sus permisos, donde se controla acceso al recurso, cambio de la clave, uso de la clave, estos procedimientos no se documentan a decir del administrador por cuanto quitan tiempo, el informe de los resultados y novedades del chequeo se envía por correo a gerencia.

3.3.4. Correo Electrónico.

En el servidor el correo se administra con WebMin, que es una herramienta de software libre, la misma que presenta facilidad de uso y seguridad, el encargado de su configuración es el administrador.

Se chequea que la configuración sea eficiente cuando se da de alta una cuenta o pasando un día, ocasionalmente se han detectado errores. La herramienta con la que los usuarios leen sus mails internamente es OUTLOCK y externamente AQUARREMAIL, lo realizan desde sus PCs.

En estas herramientas se encuentra habilitada la vista previa, confirmación de lectura, chequeo de virus en correo entrante y saliente, controles Activex y Scripts, cada usuario tiene su propia cuenta de spam y control para ciertos tipos de archivos, por ejemplo: .exe El servidor automáticamente baja los mails de toda la empresa a sus discos y los reparte a sus destinos, los mails no se borran del servidor. No existen mecanismos de filtrado dentro del encabezado o cuerpo del mensaje para evitar virus o correos no deseados. En cuanto al

espacio en disco se asigna espacio a cada usuario y a cada cuenta de mail, la cantidad varía de acuerdo al perfil y grupo.

Nunca ha sucedido que se llegue al límite de espacio en disco asignado. Solo algunos empleados tienen direcciones de mail, esto depende del perfil del empleado, con el mismo mail interno se tiene acceso al mail externo. El mail interno va directamente al servidor de correos, se monitorea esporádicamente para controla que los usuarios no usan el mail para fines personales. Además se controlan los Spams en estas direcciones.

Solo personal autorizado puede hacer uso del Chat para esto se usa MSN, internamente se lo realiza con LANMESSENGER, se permite bajar archivos solo internamente con LANMESSENGER, cuando se necesita usar programas de file sharing se utiliza FTP seguro.

Por política de la empresa se prohíbe el envío de archivos u otros documentos confidenciales vía mail. Se utiliza TOKEN para las transacciones, estos se usan para mensajes externos, la clave es privada sin embargo la utilizan las secretarias para enviar mensajes a nombre de sus jefes.

3.3.5. Control de Virus.

En la empresa no ha habido problemas graves por infección de virus, en parte porque en las PCs se encuentra habilitado sólo los procesos que el usuario utiliza para su trabajo, inclusive está deshabilitada la unidad de disco C. En cuanto a los correos se cuenta con buenas protecciones para evitar el ingreso de virus por este medio.

La empresa cuenta con el antivirus MAILSCANNER en el servidor de internet, el mismo que se ejecuta continuamente y controla el correo entrante y saliente, en el servidor como en las Pcs se realiza el respaldo mediante una imagen de disco.

Mailscannner es un antivirus de software libre, que se actualiza automáticamente, tanto los servidores como las PCs tiene instalado el antivirus.

El escaneo en busca de archivos infectados por virus se lo realiza a diario automáticamente, además el firewall y el antivirus están relacionados y son compatibles entre sí.

3.3.6. Muros de fuego (Firewall).

El firewall que se usa es el IPT que se encuentra en el servidor de internet, es del tipo gateway de filtrado de paquetes (packet filtering gateways), utiliza la política de configuración se especifica solo lo que está permitido y se prohíbe todo lo demás.

Está configurado para discriminar entre tres clases de paquetes:

- paquetes entrantes a la red
- paquetes salientes de la red
- paquetes en tránsito

Tiene habilitados los servicios HTTP, SCH, BUFTPD y deshabilitados todos los demás, soporta autenticación, incluye las direcciones NAT en la autenticación, usa password. Incluye registro de intentos no autorizados de ingreso, genera logs, provee reportes, no tiene alarmas.

Es completamente escalable, tiene buen desempeño, es fácil de configurar, es fácil de usar, fácil de mantener, tiene buen servicio postventa; nunca ha ocurrido una caída del firewall .

Se encuentran deshabilitados completamente los servicios o protocolos: SUID, RLOGIN, RSH, REXEC, SU, NetStar, GOPHER, TFTP, Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY.

3.3.7. Control de Ataques a la Red.

Ataques de Red

La empresa no dispone de herramientas para prevenir los ataques de red, debido a que no se ha presentado ningún ataque hasta el momento.

Aunque la zona desmilitarizada provee una buena protección contra intentos de acceso hacia el resto de la red local de la empresa; no se ha instalado una, principalmente debido al costo en hardware y software que esto implica.

Sistema de Detección de Intrusos (IDS - Intrusion Detection System)

En la empresa no se han registrado intrusiones, no hay herramientas para detección de intrusos, solo cuentan con la configuración del firewall.

Negación de servicio (DOS - Denial Of Service)

No se han implementado controles con respecto a la ocurrencia de DOS. No existen herramientas para la detección. En Linux, el kernel está configurado para reconocer ciertos tipos de ataques de denegación se servicios (DOS) como:

- Ping of Death.
- Spoofing

No existe ninguna herramienta anti-spoofing. No se configura el acceso externo para que el firewall explícitamente deniegue cualquier tráfico de la red externa que posea una dirección fuente que debería estar en el interior de la red interna.

Ataque a los Passwords El archivo de los passwords del sistema se almacena en el directorio /etc/passwd. Este archivo está en texto plano y puede ser accesible ya que no está encriptado.

3.4. Seguridad de las aplicaciones.

3.4.1. Software.

Nuevamente basado en la experiencia del Administrador del CPD, para elegir los sistemas operativos y programas usados en la empresa se considero: los requerimientos funcionales, de compatibilidad, de desempeño, de interoperabilidad, fiabilidad, facilidad de uso, costo de mantenimiento.

También se consideraron aspectos de seguridad como: identificación y autenticación, control de acceso, incorruptibilidad, fiabilidad, seguridad de las transmisiones, backup de datos, entre otros.

Una vez analizados estos aspectos se tomó la decisión de cual sistema operativo y programas se instalaran.

3.4.2. Bases de datos.

Los archivos de las Bases de Datos cuentan con control de acceso, realizando los siguientes controles: número de conexiones a bases de datos, generación de nuevos objetos de bases de datos, modificación de bases de datos. De igual manera se hace chequeos regulares de la seguridad de la base de datos, el acceso a los archivos de la BD los sistemas operativos y a las tablas del sistema además del administrador lo tienen dos funcionarios del departamento de sistemas.

No existen usuarios que tengan los mismos permisos que el administrador, la base de datos tiene suficientes recursos libres para trabajar, los registros de las bases de datos cuando un usuario los elimina se marcan como borrados para su posterior eliminación.

3.4.3. Aplicaciones en PC's.

Todas las PCs de la empresa tienen instalado los mismos programas con las mismas versiones, los mismos que fueron autorizados por el departamento de sistemas, así mismo todas las PCs tienen una configuración estándar.

Existe un procedimiento para instalar aplicaciones en las máquinas de los usuarios, así como para la instalación o actualización de parches en las aplicaciones, estos procesos son realizados exclusivamente por el asistente de sistemas y es documentado mediante bitácoras.

De igual forma existe un procedimiento para encontrar programas que no deberían estar en las máquinas, para lo cual se utiliza la herramienta BELARC.

Los usuarios tienen acceso a internet de acuerdo a perfiles, es prohibido instalar software y aplicaciones bajadas de la web como versiones de prueba o demos.

3.4.4. Datos de las aplicaciones.

En las aplicaciones desarrolladas dentro de la empresa se implementan controles sobre los datos de entrada que permiten asegurar su integridad, exactitud y validez; con los datos de salida se han implementado ciertas restricciones como deshabilitar el portapapeles, se permite realizar impresiones solo a los usuarios que por su perfil tengan que hacerlo, se deshabita todo lo que no tenga que ver con su puesto de trabajo, incluso en el área de producción está deshabilitada incluso la unidad C; por política de la empresa no se permite el usos de laptops.

Por seguridad los archivos de programas y los de trabajo se almacenan en directorios separados, el acceso a las librerías de programas es limitado.

3.4.5. Ciclo de Vida.

La empresa cuenta con aplicaciones propias desarrolladas por el departamento de sistemas para cada área de empresa, se aplica la metodología de desarrollo conocida como YOURDON, que a según el administrador del CPD es una de las tres metodologías de

diseño estructurado más utilizadas, completo, práctico, orientado a objetos y adecuado para proyectos comerciales.

Para el diseño con la metodología Yourdon se debe seguir los siguientes pasos básicos: diagrama de flujos, diagrama de estructura, evaluar el diseño, preparar el diseño para la implementación, diseño físico y lógico.

Las necesidades de las aplicaciones a desarrollar se expresan a través de reuniones de trabajo con el personal del área que solicita la aplicación, estas necesidades se plasman en un documento. Antes de iniciar con el desarrollo se realiza un análisis de riesgos, en caso de trabajar con terceros esta debe sujetarse a la reglamentación establecida para el efecto.

Las aplicaciones se implementan en POWERBUILDER v. 10.5, durante la implementación se realiza validación de datos y pruebas de acceso a través de menús. Para las pruebas se generan planes de pruebas, se realizan pruebas por módulos, para lo cual se generan escenarios, no se documentan las pruebas y sus resultados en papel, solo a través de informes por correo.

En la instalación y mantenimiento no se usa ninguna metodología específica, simplemente queda a criterio de la persona de sistemas designada para el efecto.

En cuanto a la documentación de los sistemas desarrollados en ella se incluye: generalidades del sistema, fecha de implementación, responsable, objetivos, diagramas general y de funciones, de diseño de registros; documentación de los programas: objetivos, diagrama de flujo y archivos de entrada y salida.

Manual de operación, manual del usuario por procesos, manual de características de seguridad, descripción del hardware y software, políticas, estándares, procedimientos, backup, descripción del usuario y del operador del sistema.

En el caso de que se compre el sistema primero se establece la funcionalidad, la disponibilidad del proveedor y un análisis costo beneficio, al comprar el sistema se exige la documentación del mismo.

3.5. Administración CPD.

3.5.1 Administración del CPD.

Las responsabilidades puntuales son asignadas a cada empleado, estas responsabilidades para las funciones de TI son realizadas por el jefe de sistemas. El encargado de la seguridad y de las políticas de seguridad y administración es el jefe de sistemas. Es quién realiza la planificación y asigna las tareas a los empleados del CPD.

El administrador de sistemas es el encargado de informar a los altos ejecutivos sobre las actividades en el CPD, estos se realizan periódicamente a través del correo interno de la empresa, no existe documentación impresa de los mismos.

Se han desarrollado planes formales a corto y largo plazo del departamento de sistemas, se aplican políticas, normas, estándares y procedimientos para la planificación, el control y la evaluación de las actividades del área de sistemas, estos han sido desarrollados por el jefe de sistemas en base a reuniones donde se analizan las prioridades de la empresa.

Cuando se ingresa un nuevo empleado al CPD, mientras se encuentra en la etapa de capacitación no se le asignan todos los permisos, sino que se los va abriendo de acuerdo al avance en la capacitación hasta completar todos sus permisos de cuerdo al perfil del puesto, estos permisos son asignados por el administrador de sistemas. No existe diferencia entre los permisos de los desarrolladores y los administradores.

Los altos funcionarios están conscientes de la importancia de la seguridad, porque en base a sus requerimientos se han desarrollado los sistemas de la empresa, razón por la cual son ellos los que exigen se cumplan estrictamente las normas de seguridad. El resto de empleados conocen y se han capacitado en seguridad pero no son plenamente conscientes de su importancia.

3.5.2. Capacitación.

Las nuevas normas de seguridad se dan a conocer a través de charlas y reuniones con los empleados, lo que ha dado buen resultado hasta el momento por cuanto todos conocen lo que hay que hacer para garantizar las seguridad.

Cuando ingresa un empleado nuevo a la empresa se lo capacita en el uso del sistema, en esta charla se incluye consideraciones sobre seguridad como:

- no usar passwords fáciles de descifrar
- no divulgarlas
- no escribirlas ni guardarlas bajo el teclado o cerca de la PC.
- el password es el principal método de seguridad del sistema.
- no modificar la configuración de las PCs
- no abrir correos de origen desconocido.

No existe ningún documento de consentimiento por parte de los usuarios para que se auditen sus actividades en el sistema, ni declaraciones que conocen las normas de seguridad y buen uso.

3.5.3. Backups.

Los backups se realizan diariamente, es un proceso que se lo realiza automáticamente mediante programación Bash Shell y tareas programadas el mismo que está a cargo del administrador de sistemas.

Estos backups son normales, se almacenan en Disco Duro y CDs, cada seis meses se graba la información en CDs y se entregan tres copias: una a Gerencia, una a Auditoría Interna y una al Jefe de Sistemas. Los backups se almacenan dentro y fuera de la empresa en lugares seguros, en la documentación escrita de los backups solo se anota la fecha de realización.

La empresa no posee información en la Web, solo cuenta con páginas estáticas de las cuales si existe respaldo.

No se hace ningún backup de los logs del sistema, solo se los almacena y depura periódicamente.

3.5.4. Documentación.

En el centro de procesamiento de datos existe documentación sobre:

- Actividades que se desarrollan normalmente
    - los procesos a realizar.
    - los controles que se efectúan.
    - las relaciones con otras áreas.
    - mecanismos de distribución de la información.
- Documentación detallada sobre el equipamiento.

- distribución física (PCs, equipos y puestos de trabajo)
- inventario de hardware y software.
- número de serie del hardware.
- número de licencia de software.
- inventario de insumos.
- ubicación de nodos.

Se cuenta con una documentación del Plan de contingencia, Plan de seguridad, manuales de procedimientos del CPD, manuales de usuario por procesos, manuales del sistema, manuales de operación, manuales de seguridad.

3.6. Evaluación del Plan de Seguridad Informática.

3.6.1. Plan de seguridad.

No existe un Plan de Seguridad establecido formalmente, solo se cuenta con las normas y controles establecidos para los diferentes aspectos anteriormente analizados como seguridad física, seguridad lógica, de las aplicaciones, de la red, administración. Todas estas normas y controles no se encuentran documentados y condensados de manera adecuada en un plan de seguridad, que contenga como mínimo:

- Objetivo General
- Objetivos Específicos
- Vigencia del Plan

Existe un plan de contingencias desarrollado por el administrador de sistemas, el mismo que se lo desarrollo previo un análisis de riesgo, se tomó en cuenta no solo al área de sistemas sino a todas las áreas de la empresa, esto considerando que todos los sistemas están completamente integrados.

Este incluye un Plan de reducción de riesgos, se posee las acciones defensivas en caso de violación interna y/o externa, acciones tales como desconectar los servidores, cerrar los accesos, rastrear al intruso, entre otras. Los responsables del plan de contingencias y usuarios reciben la debida capacitación y entrenamiento sobre su aplicación, el plan se mantiene actualizado de acuerdo a nuevos puestos, funciones y amenazas. Sin embargo el mismo no se documenta, no existe un documento que detalle:

- Objetivo

- Modo de ejecución
- Tiempo de duración
- Costes estimados
- Recursos
- Evento que dispara el plan
- Personas encargadas de ejecutar el plan
- Administración de Incidentes

No se cuenta con un Plan de Respuesta a incidentes, la respuesta a incidentes de seguridad se la realiza a criterio del administrador de sistemas, esto lo realiza de acuerdo a los siguientes pasos:

- Detección del incidente
- Análisis del incidente
- Contención, erradicación y recuperación

Este procedimiento tampoco es documentado formalmente, el administrador se limita a informar de lo realizado a través del correo.

3.6.2. Backup de equipos.

En caso de que el servidor de internet de fibra óptica falle se utiliza el servidor de internet satelital, con lo que se garantiza las comunicaciones con los clientes. La información de cada servidor es respaldada en discos externos, si un disco falla se puede trabajar con el disco externo hasta realizar la reparación o reposición del disco dañado.

El hardware se encuentra asegurado por lo que no se cuenta con backups del mismo, ya que la aseguradora se encarga de su reparación o reposición.

No se cuenta con un centro de procesamiento de datos alternativo, ya que de acuerdo a información del administrador no se justifica esta inversión; los servidores se encuentran en una sola habitación.

3.6.3. Recuperación de Desastres.

A pesar de existir la conciencia de los beneficios de contar con un plan de recuperación, este no se ha desarrollado.

El personal del CPD conoce lo que debe hacerse antes, durante y después del desastre sin embargo manifiestan que no lo han realizado por falta de tiempo y recursos humanos para destinarlos a esta tarea.

CAPÍTULO IV
ANÁLISIS DE LA INFORMACIÓN.

4.1. Evaluación del Nivel de Madurez y Nivel de Riesgo.

Para la evaluación de los niveles de madurez se ha tomado como base el modelo genérico de madurez de Cobit 4.1.

4.1.1. Modelo Genérico de Madurez.

Este modelo genérico de madurez evalúa el nivel en el que se encuentran los controles implementados por la administración para garantizar la seguridad de la información.

Tabla 10.

Niveles de Madurez Cobit 4.1.

Nivel	Descripción
0 No Existe	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Fuente: IT. Gobernance Institute Cobit 4.1 2007.- *Marco de Trabajo, Objetivos de Control, Directrices Generales, Modelos de Madurez (p.19)*

.

4.1.2. Nivel de Riesgo.

De igual manera para determinar el riesgo se ha tomado en consideración las matrices:

- De determinación de impactos, para cuantificar el impacto relacionado a un evento de acuerdo a un criterio relacionado a la gravedad del evento.
- De determinación de probabilidad de ocurrencia, para cuantificar la posibilidad de que ocurra un evento en el transcurso de un periodo determinado.
- De evaluación de riesgos, que cuantifica el nivel de riesgo y la forma en que se debe realizar las acciones para mitigar los efectos del mismo.

Tabla 11.

Matriz de determinación de impacto.

Criterio	Impacto	Calificación
Catastrófico	1 semana o más	5
Significativo	1 día a una semana	4
Moderado	4 a 8 horas	3
Menor	1 a 4 horas	2
Insignificante	Menos de 1 hora	1

Fuente: Muñoz, A. (2014)

Tabla 12.

Matriz de determinación de la probabilidad de ocurrencia.

Criterio	Probabilidad	Calificación
Muy Probable	12 a 18 meses	5
Probable	18 a 24 meses	4
Posible	Ocurrirá en algún momento	3
Poco Probable	En algún momento	2
Muy Poco Probable	Menos de 1 hora	1

Fuente: Muñoz, A. (2014)

Tabla 13.

Matriz de evaluación de riesgos.

Riesgo	Descripción	Ponderación
Alto	Acción inmediata	Mayor o igual a 15
Moderado	Acción mediata	Mayor a 5 Menor a 15
Bajo	Acción eventual	Menor a5

Fuente: Muñoz, A. (2014)

4.2. Análisis por Dominios de Cobit 4.1

Tabla 14.

Análisis Dominio Planificar y Organizar.

Código	Proceso	Actividad	Resultado Entrevista	Nivel Madurez	Impacto	Probabilidad Ocurrencia	Calificación del Riesgo
PO1	Definir el Plan estratégico de TI	Determinar la existencia de un Plan Estratégico de TI	No existe Planeación Estratégica de TI. Existe conciencia sobre la necesidad de una Planeación estratégica.	1	4	5	20 Alto

PO2	Definir la arquitectura de la información	Verificar la existencia de un modelo de datos que garantice la integridad y consistencia de los datos.	Se reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de la arquitectura ocurre de manera ad hoc.	1	3	2	6 Moderado
PO3	Determinar la dirección tecnológica	Existe un Plan de infraestructura tecnológica, arquitectura y estándares que aprovechen las oportunidades tecnológicas?	No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. No existe el conocimiento y experiencia para desarrollar dicho plan.	0	3	2	6 Moderado
PO4	Definir los procesos, Organización y Relaciones de TI	La estructura organizacional de TI es flexible y adaptable, existe un proceso de mejora continua?	La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, no existe un proceso de mejora continua. Existe dependencia de individuos clave.	2	3	3	9 Moderado
PO5	Administrar la inversión en TI	Existe un portafolio de inversión en TI y seguimiento de presupuestos de TI de acuerdo a la estrategia de TI.?	Se reconoce la necesidad de administrar la inversión en TI, la asignación se hace ad hoc, existe documentación informal.	1	3	3	9 Moderado
PO6	Comunicar las aspiraciones y la Dirección de la Gerencia.	Determinar la existencia de un ambiente de control de la información, la conciencia de la seguridad de información; existen políticas de comunicación.	Se ha estructurado un ambiente de control, con la determinación de políticas, procedimientos y estándares de seguridad de la información.	3	3	2	6 Moderado
PO7	Administrar los Recursos Humanos de TI.	Existe un proceso para adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio.?	Existe un proceso documentado para administrar los recursos humanos de TI, plan de administración de recursos, y un plan de entrenamiento.	3	2	3	6 Moderado
PO8	Administrar la calidad	Se debe elaborar y mantiene un sistema de administración de calidad. ? Existe un sistema de administración de calidad?	Existe conciencia por parte de la dirección de la necesidad de un Sistema de administración de la calidad. El mismo es impulsado por individuos . No existe documentación.	1	3	3	9 Moderado

PO9	Evaluar y Administrar los riesgos de TI.	Determinar la existencia de un marco de trabajo de administración de riesgos.	No existe un documento formal sobre administración de riesgos, la administración de riesgos se la realiza de acuerdo a la experiencia del administrador del CPD.	1	4	4	16 Alto
PO10	Administrar Proyectos	Se ha establecido un marco de trabajo de administración de programas y proyectos. El marco de trabajo garantiza la correcta asignación de prioridades y la coordinación de todos los proyectos?	Las técnicas y enfoques de administración de proyectos es una decisión individual, no existe compromiso de la alta gerencia, no se hace seguimiento al tiempo y a los gastos del proyecto comparado con el presupuesto.	1	3	3	9 Moderado

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que de los 10 procesos del Dominio Planificar y Organizar, los niveles de madurez de Cobit 4.1 se distribuyen de la siguiente forma:

Tabla 15.

Distribución niveles de madurez dominio PO		
Nivel	**Número Procesos**	**Porcentaje**
0	1	10
1	6	60
2	1	10
3	2	20

Fuente: Muñoz, A. (2014)

Por lo que el Dominio Planificar y Organizar se encuentra en el Nivel de Madurez 1 de Cobit 4.1 (**Inicial**: Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.)

En la evaluación de riesgos, de los 10 procesos de Planificar y Organizar:

Tabla 16.

Distribución de riesgos dominio PO		
Nivel	**Número Procesos**	**Porcentaje**
ALTO	2	20
MEDIO	8	80
BAJO	0	0

Fuente: Muñoz, A. (2014)

Es decir 2 procesos requieren una acción correctiva inmediata y 8 procesos una acción correctiva mediata.

Tabla 17.

Análisis Dominio Adquirir e Implementar.

Código	Proceso	Actividad	Resultado Entrevista	Nivel Madurez	Impacto	Probabilidad Ocurrencia	Calificación del Riesgo
AI1	Identificar Soluciones Automatizadas	Identificar procedimientos que permitan la identificación de soluciones técnicamente factibles y rentables	No existen procedimientos definidos, se identifican las soluciones en base al criterio del administrador, existe un análisis estructurado mínimo de la tecnología existente	1	3	3	9 Moderado
AI2	Adquirir y mantener el Software	Verificar si las aplicaciones se construyen de acuerdo a los requerimientos del negocio, a tiempo y a un costo razonable.	Existe un procedimiento claro y definido que se ajusta a los requerimientos del negocio, con mecanismos de aprobación que garantizan que se sigan todos los pasos.	4	2	1	3 Bajo
AI3	Adquirir y mantener la infraestructura tecnológica	Se cuenta con planes para adquirir, implantar y mantener la infraestructura tecnológica	No existe un plan en conjunto, aunque se tiene consciencia de que la infraestructura de TI es importante. El mantenimiento se lo realiza cuando se lo necesita. No se realizan pruebas.	1	3	3	9 Moderado
AI4	Facilitar la operación y uso	Determinar la existencia de documentación para transferencia de información.	La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados.	1	3	3	9 Moderado
AI5	Adquirir recursos de TI	Existen procedimientos de control de proveedores y de adquisición de software.	Existen políticas y procedimientos de adquisición de TI de acuerdo al proceso general de adquisiciones.	3	2	2	4 Bajo

AI6	Administrar cambios	Existe un procedimiento que permita, registrar, evaluar y autorizar los cambios en la infraestructura y en las aplicaciones	No, los cambios se los realiza de acuerdo a la necesidad y de acuerdo a la experiencia del administrador, no se documentan los cambios.	1	3	3	9 Moderado
AI7	Instalar y acreditar soluciones	Determinar si se efectúan pruebas de las soluciones de aplicaciones e infraestructura.	Existe conciencia de la importancia de efectuar pruebas a la soluciones de TI, no se basa en ninguna metodología. Hay un proceso de acreditación informal.	2	3	3	9 Moderado

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que de los 7 procesos del dominio Adquirir e Implementar, los niveles de madurez de Cobit 4.1 se distribuyen de la siguiente forma:

Tabla 18.

Distribución niveles de madurez dominio AI		
Nivel	**Número Procesos**	**Porcentaje**
1	4	57.14
2	1	14.28
3	1	14.28
4	1	14.28

Fuente: Muñoz, A. (2014)

Por lo que el Dominio Adquirir e Implementar se encuentra en el Nivel de Madurez 1 de Cobit 4.1 (**Inicial**: Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.)

En la evaluación de riesgos, de los 7 procesos de Adquirir e Implementar se clasifican:

Tabla 19.

Distribución de riesgos dominio AI		
Nivel	**Número Procesos**	**Porcentaje**
ALTO	0	0
MEDIO	5	71.42
BAJO	2	28.57

Fuente: Muñoz, A (2014).

Es decir 5 procesos requieren una acción correctiva inmediata y 2 procesos una acción correctiva eventual.

Tabla 20.

Análisis Dominio Entregar y Dar Soporte

Código	Proceso	Actividad	Resultado Entrevista	Nivel Madurez	Impacto	Probabilidad Ocurrencia	Calificación del Riesgo
DS1	Definir y Administrar los niveles de servicio	Determinar si existe una definición documentada y un acuerdo de servicios de TI y de niveles de servicio.	Hay conciencia de la necesidad de administrar los niveles de servicio, el proceso es informal y reactivo. La responsabilidad y la administración de servicios no está definida.	1	3	3	9 Moderado
DS2	Administrar los servicios de terceros	Verificar si se aseguran que los servicios provistos por terceros cumplan con los requerimientos del negocio	Existe un proceso informal de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios.	2	3	3	9 Moderado
DS3	Administrar el desempeño y la capacidad	Existe un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	Cualquier medición de desempeño se basa en las necesidades de TI y no en las necesidades del cliente.	2	3	3	9 Moderado
DS4	Garantizar la continuidad del servicio	Determinar si existe un proceso efectivo de continuidad de servicios que minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI	Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas	3	4	3	12 Moderado

DS5	Garantizar la seguridad de los sistemas	Existe un proceso de administración de administración de la seguridad	Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada.	1	4	4	16 Alto
DS6	Identificar y asignar costos	Determinar si se cuenta con un sistema justo y equitativo para asignar costos de TI al negocio	Hay una completa falta de cualquier proceso reconocible de identificación y distribución de costos en relación a los servicios de información brindados	0	3	3	9 Moderado
DS7	Educar y entrenar a los usuarios	Existe un programa organizado de entrenamiento a los usuarios de TI.	Hay conciencia de la necesidad de capacitar a los usuarios, sin embargo el proceso es reactivo e informal.	2	4	4	16 Alto
DS8	Administrar la mesa de servicio y los incidentes	Se ha instalado y está en operación una mesa de servicios, monitoreo y reporte de tendencias.	No hay soporte para resolver problemas y preguntas de los usuarios. Hay una completa falta de procesos para la administración de incidentes. La organización no reconoce que hay un problema que atender.	0	3	3	9 Moderado
DS9	Administrar la configuración	Determinar si se llevan a cabo tareas que garanticen la seguridad de las configuraciones de hardware y software.	Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de hardware y software pero de manera individual. No están definidas prácticas estandarizadas.	1	3	4	12 Moderado

DS10	Administrar los problemas	Identifican y clasifican los problemas, analizan sus causas y se registran las soluciones.	Algunos individuos expertos brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas.	1	3	4	12 Moderado
DS11	Administrar los datos	Mantener la integridad, exactitud, disponibilidad y protección de los datos	Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y seguridad.	3	4	2	8 Moderado
DS12	Administrar el ambiente físico	Verificar que las instalaciones estén bien diseñadas y bien administradas	El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla	5		1	4 Bajo
DS13	Administrar las operaciones	Determinar si existe una efectiva administración del procesamiento de datos y del mantenimiento de hardware.	Las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y la propiedad está asignada. La gerencia monitorea el uso de los recursos de cómputo y la terminación del trabajo o de las tareas asignadas	4	4	1	4 Bajo

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que de los 13 procesos del dominio Entregar y Dar Soporte; los niveles de madurez de Cobit 4.1 se distribuyen de la siguiente forma:

Tabla 21.

Distribución niveles de madurez dominio DS		
Nivel	**Número Procesos**	**Porcentaje**
0	2	15.38
1	4	30.76
2	3	23.07
3	2	15.38
4	1	7.69
5	1	7.69

Fuente: Muñoz, A. (2014)

Por lo que en promedio el Entregar y Dar Soporte se encuentra en el Nivel de Madurez 2 de Cobit 4.1 (**Repetible:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.)

En la evaluación de riesgos, de los 13 procesos de Entregar y Dar Soporte se clasifican como:

Tabla 22.

Distribución de riesgos dominio DS		
Nivel	**Número Procesos**	**Porcentaje**
ALTO	2	15.38
MEDIO	9	62.23
BAJO	2	15.38

Fuente: Muñoz, A (2014).

Es decir 2 procesos requieren acciones correctivas inmediatas, 9 procesos acciones correctivas mediatas y 2 procesos acciones correctivas eventuales.

Tabla 23.

Análisis Dominio Monitorear y Evaluar.

Código	Proceso	Actividad	Resultado Entrevista	Nivel Madurez	Impacto	Probabilidad Ocurrencia	Calificación del Riesgo
ME1	Monitorear y Evaluar el desempeño de TI	Definir si existe un proceso para monitorear y reportar las métricas del proceso e identificar e implementar acciones de mejoramiento del desempeño	La organización no cuenta con un proceso implantado de monitoreo. No se cuenta con reportes útiles, oportunos y precisos.	0	3	3	9 Moderado

ME2	Monitorear y evaluar el control interno	Determinar si existe un proceso definido de control interno	La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc.	1	3	3	9 Moderado
ME3	Garantizar el cumplimiento regulatorio	Se cumplen las leyes y regulaciones.	Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización.	1	3	3	9 Moderado
ME4	Proporcionar el Gobierno de TI	El gobierno de Ti está alineado con los objetivos empresariales	La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio.	1	4	3	12 Moderado

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que de los 4 procesos del dominio Monitorear y Evaluar; los niveles de madurez de Cobit 4.1 se distribuyen de la siguiente forma:

Tabla 24.

Distribución niveles de madurez dominio ME		
Nivel	**Número Procesos**	**Porcentaje**
0	1	15.38
1	3	30.76

Fuente: Muñoz, A. (2014)

Por lo que el dominio Monitorear y Evaluar se encuentra en el Nivel de Madurez 1 de Cobit 4.1 (**Inicial**: Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.)

Tabla 25.

Distribución de riesgos dominio ME		
Nivel	**Número Procesos**	**Porcentaje**
ALTO	0	0
MEDIO	4	100
BAJO	0	0

Fuente: Muñoz, A. (2014)

En la evaluación de riesgos, de los 4 procesos de Monitorear y Evaluar se clasifican como de riesgo moderado 4 procesos; es decir requieren de acciones correctivas mediatas.

Niveles de madurez de los 34 procesos de Cobit.

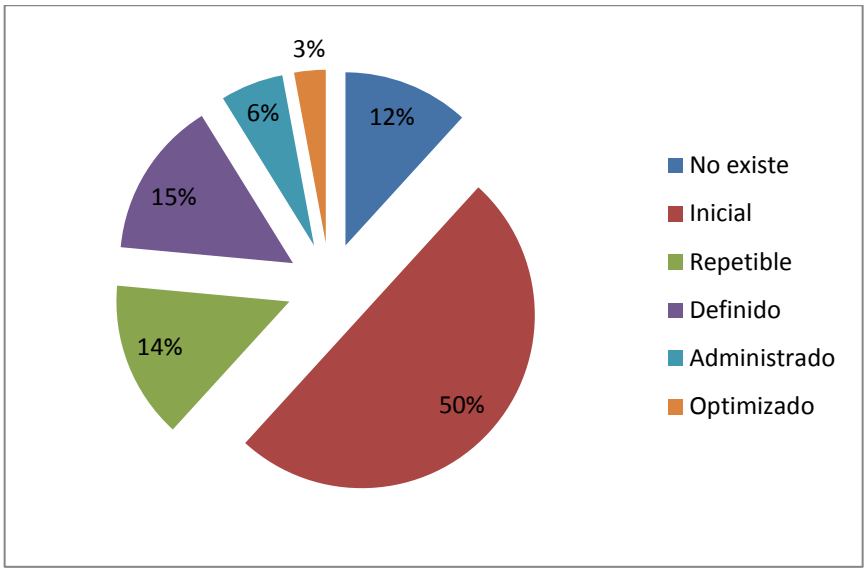


Figura 9: Distribución de los niveles de madurez de los 34 procesos de Cobit 4.1.
Fuente : Muñoz, A. (2014)

Analizando los 34 procesos de Cobit 4.1 se puede establecer que el nivel de madurez en el que se encuentra la empresa es el **nivel 1 Inicial**, es decir existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

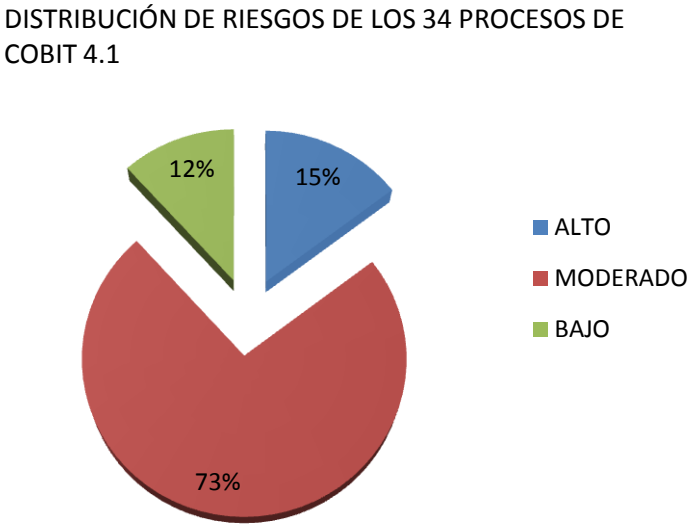


Figura 10: Distribución de Riesgos de los 34 procesos de Cobit 4.1.
Fuente: Muñoz, A. (2014)

En lo relaciona lo al nivel de riesgo de los 34 procesos de Cobit 4.1, se ha determinado que el 15% de los procesos han sido clasificados como de alto riesgo por lo que la empresa necesita actuar inmediatamente en la aplicación de las recomendaciones establecidas; el 73% de procesos se encuentran clasificados como de riesgo moderado, es decir son procesos que requieren una acción mediata en la aplicación de las recomendaciones.

4.3. Análisis por componentes.

Tabla 26.

Análisis Seguridad Física.

Elemento	Actividad	Resultado Entrevista	Debilidad	Nivel de Madurez	Impacto	Probabilidad Ocurrencia	Calificación del Riesgo
Equipamiento	Definir si los equipos instalados responden a las necesidades del negocio.	Los equipos han sido adquiridos de acuerdo a un estudio previo de las necesidades de la empresa; las características de los mismos fueron fijadas de acuerdo a la experiencia del administrador.	No se encontraron debilidades significativas	3	1	1	1 Bajo

Control de acceso Físico al CPD	Verificar los controles de acceso al CPE	En la instalación del CPD no se hizo un análisis costo beneficio para determinar los controles de acceso físico necesarios. Actualmente ya se cuenta con el área destinada al área de sistemas y se implementó el control de acceso basado en la experiencia del administrador, el acceso al área de servidores es solo para el personal de sistemas.	No se encontraron debilidades significativas	2	4	2	8 Moderado
		Se restringe el acceso al CPD a las personas que no pertenecen al mismo, utilizando tarjetas de entrada, en la garita de ingreso y áreas de la planta. Guardias de seguridad, en la garita de entrada. Circuito cerrado de televisión, en todas las áreas productivas y para control de los exteriores de la empresa.	No existe una cámara del circuito cerrado de televisión que grabe específicamente la puerta de entrada del mismo.	3	4	4	16 Alto
		Se les permite el ingreso solo si trae la tarjeta de proximidad, si la persona no la trae, tiene que ir a recursos humanos para que le entreguen una, caso contrario no puede trabajar ya que tiene que timbrar en los relojes internos de planta. En el caso de personas ajenas a la empresa el guardia de la entrada acompaña al visitante hasta la oficina donde es recibido por el empleado; al finalizar la visita el empleado acompaña al visitante hasta la garita de guardias.	No se encontraron debilidades significativas	3	3	2	6 Moderado
Control de acceso a los Equipos	Confirmar la existencia de controles de acceso a los equipos.	El acceso a los equipos se controla mediante una clave habilitada en la BIOS, las máquinas no cuentan con CD's ni lectoras de memoria o están deshabilitados. Nunca se pide CD ROM ni lectores de tarjetas. Existen programas que bloquean la entrada de dispositivos USB.	No se encontraron debilidades significativas	3	4	3	12 Moderada
		Los dispositivos extraíbles se guardan en gabinetes con llave en un lugar apropiado fuera del alcance del personal y con las medidas de seguridad que garanticen su correcto funcionamiento, las llaves de los gabinetes las tiene el administrador bajo su custodia. El técnico de sistemas realiza el control de los dispositivos que se instalan en las PC's de acuerdo al cronograma previamente establecido aproximadamente cada tres meses.	No se encontraron debilidades significativas	3	4	2	8 Moderada

		Si existe control permanente, un funcionario del CPD acompaña al técnico de mantenimiento contratado durante su permanencia en el mismo, una vez terminado el trabajo lo escolta a la salida y reporta el trabajo realizado.	No se encontraron debilidades significativas	3	4	3	12 Moderado
		No, no se ha dado el caso de entradas no autorizadas en las PCs, los puertos no usados están deshabilitados.	No se encontraron debilidades significativas	3	4	3	12 Moderado
		No puede nadie instalar impresoras o unidades removibles; en el caso de ser necesario se lo debe solicitar al departamento de sistemas.	No se encontraron debilidades significativas	3	4	3	12 Moderado
		Para verificar que no se hayan instalado dispositivos en las PCs se espera al mantenimiento preventivo, el mismo que está previamente programado y es periódico, esto lo realizan los técnicos de sistemas, cada tres meses.	No se encontraron debilidades significativas	3	4	3	12 Moderado
		Los servidores de la empresa permanecen prendidos las 24 horas del día de lunes a domingo, es necesario debido a que el trabajo en la planta se lo realiza en turnos que cubren las 24 horas del día.	No se encontraron debilidades significativas	4	3	3	9 Moderado
		No se cuenta con un servidor de repuesto o redundante, cada servidor tiene discos redundantes.	Es peligroso el no contar con un servidor de repuesto en caso de una falla del servidor principal.	0	4	4	16 Alto
Dispositivos auxiliares	Identificar los equipos auxiliares y soporte instalados en el CPD	La empresa cuenta con los siguientes dispositivos de soporte para el equipamiento informático: Aire acondicionado.- El CPD cuenta con aire acondicionado el mismo que mantiene la temperatura entre los 18 y 20º que es lo recomendado por lo proveedores de equipos. Extintores de incendios	El CPD no cuenta con alarmas contra fuego, humo e intrusos.	3	4	3	12 Moderado
		En el CPD hay 4 unidades de poder ininterrumpido de 6 Kva cada una, con un banco de baterías de una hora de duración los mismos que funcionan todo el tiempo.	No se encontraron debilidades significativas	4	4	2	8 Moderado
		Si existen estabilizadores de tensión eléctrica instalados	No se encontraron debilidades significativas	4	4	2	8 Moderado
		Son equipos manuales de polvo químico, se encuentran ubicados en los exteriores de las áreas, su cantidad y ubicación lo determinó Seguridad Industrial.	No se encontraron debilidades significativas	4	3	2	6 Moderado

		El departamento de mantenimiento industrial se encarga de realizar revisiones periódicas de las instalaciones y cableado eléctrico de la empresa.	No se encontraron debilidades significativas	4	3	3	9 Moderado
		No se cuenta con rociadores, no se ha dado ninguna emergencia en la que se haya necesitado utilizar los extintores; al ser de polvo químico no sería necesario cubrir los equipos.	No se encontraron debilidades significativas	4	3	3	9 Moderado
		Si, existe una red eléctrica industrial 220V para el área de planta y una red eléctrica de 110V para las áreas administrativas.	No se encontraron debilidades significativas	4	3	2	6 Moderado
		El CPD cuenta con equipos que evitan la sobrecarga de la red eléctrica	No se encontraron debilidades significativas	4	3	2	6 Moderado
		Si se tiene hardware especial de aislamiento y protección de dispositivos magnéticos.	No se encontraron debilidades significativas	4	3	1	3 Bajo
Edificio	Conocer si el espacio físico destinado al CPD cumple los requisitos mínimos.	El área donde se encuentra el CPD está ubicado en un área lo suficientemente grande previendo el crecimiento futuro de la red, cuenta con techo falso y pisos para pasar el cableado de fácil acceso, elaborados con materiales impermeables e incombustibles al igual que las paredes.	No se tomó en consideración las medidas de seguridad para los datos y equipos, el CPD no está ubicado en pisos altos, el piso y el techo no están fabricados con materiales ignífugos.	3	4	4	16 Alto
		Está ubicado en la planta baja, cerca del backbone para facilitar las conexiones, el personal que labora en el CPD está capacitado para actuar en caso de incendio, no se permite comer ni tomar bebidas, se deben seguir ciertos procedimientos estandarizados para la recepción y almacenaje de papel	No se encontraron debilidades significativas	3	4	3	12 Moderado
Cableado	Identificar si en la instalación del cableado se consideró las medidas de seguridad mínimas.	En la instalación del cableado se consideró la ubicación de los canales, para que no sean afectados por inundaciones, cortes eléctricos, desagües o campos magnéticos, para el cableado se utilizó la norma IEEE con cableado estructurado STP categoría 6; para evitar interferencia, tanto el cableado eléctrico como el de Red van entubados, y cuando van por la misma canaleta, esta tiene una división.	No se encontraron debilidades significativas	4	1	1	1 Bajo

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que las 24 actividades del componente Seguridad Física se distribuyen de la siguiente forma:

Tabla 27.

Distribución niveles de madurez Seguridad Física		
Nivel	**Número Actividades**	**Porcentaje**
0	1	4.7
1	0	0
2	1	4.7
3	12	50
4	10	41.67
5	0	0

Fuente: Muñoz, A. (2014)

Por lo que el componente Seguridad Física se encuentra en el Nivel de Madurez 3 de Cobit 4.1.(**Definido:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.)

En la evaluación de riesgos, de las 24 actividades del componente Seguridad Física se clasifican:

Tabla 28.

Distribución de riesgos Seguridad Física		
Nivel	**Número Actividades**	**Porcentaje**
ALTO	3	12.5
MEDIO	18	75
BAJO	3	12.5

Fuente: Muñoz, A. (2014)

En decir 3 actividades requieren de acciones correctivas inmediatas, 18 de acciones correctivas mediatas y 3 de acciones correctivas eventuales.

Tabla 29.

Análisis Seguridad Lógica.

Elemento	Actividad	Respuesta	Debilidad	Nivel de Madurez	Impacto	Probabilidad	Calificación Riesgo
Identificación y Autenticación	Identificar si la organización cuenta con una lista actualizada de usuarios que tienen acceso autorizado a los recursos de los Sistemas de Información, para lo cual	Los datos que se guardan en el perfil de usuario tienen relación con código de recursos humanos y la unidad a la que pertenece Recursos humanos informa las desvinculaciones y cambios de funciones del personal, existen procedimientos para la eliminación de	No se encontraron debilidades significativas No se encontraron debilidades significativas	2 3	4 4	1 1	4 Bajo 4 Bajo

debe tener determinado procedimientos de identificación y autenticación.	claves, se llevan registros de las claves eliminadas.					
	No cuentan con una política documentada para la gestión de claves de acceso, la administración de las claves es responsabilidad del personal de sistemas. Para proteger las claves se utilizan técnicas de cifrado. El tiempo de conexión no está limitado al horario de trabajo.	No se cuenta con una política documentada para la gestión de claves de acceso, esto se lo realiza basado en la experiencia del administrador de sistemas.	2	4	3	12 Moderado
	Al tipiar el password se muestran Asteriscos para evitar que el mismo sea revelado, los datos de autenticación se guardan encriptados. El acceso a estos datos es solo para el personal de sistemas, la autenticación es para toda la red y por aplicación.	No se encontraron debilidades significativas	3	4	1	4 Bajo
	No se bloquea el acceso luego de un número de intentos fallidos, el equipo espera un tiempo para mostrar nuevamente la ventana de ingreso de contraseña. No se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos pero para mensajes externos si se las usa ya que para algunos documentos son necesarias.	No se encontraron debilidades significativas	2	4	1	4 Bajo
	El usuario genera su clave, la misma que debe contener letras y números, mínimo 4 caracteres y máximo 8 caracteres, no se permite que el password tenga el nombre de la empresa o el nombre del usuario, tampoco dos cuentas pueden tener el mismo password tanto para los usuarios como para el administrador, el password no puede ser el mismo que el ID de usuario.	No se encontraron debilidades significativas	2	4	1	4 Bajo
	El password debe ser cambiado cada tres meses, si el usuario pierde o revela el password debe denunciar al departamento de sistemas. No se guardan los passwords utilizados por cada usuario, si se capacita a los usuarios sobre la administración de	No se guarda los password usados por el usuario.	4	4	1	4 Bajo

		su password.					
Roles	Verificar la existencia de un mecanismo que permita establecer que operaciones puede realizar cada usuario dentro del sistema de información	Las claves se asignan por usuario, los permisos de lectura, escritura, ejecución, eliminación, todos los anteriores) son asignados de acuerdo a las funciones del usuario. El ID hace referencia a una persona.	No se encontraron debilidades significativas	4	4	1	4 Bajo
Transacciones	Establecer controles a través de las transacciones, por ejemplo solicitar una clave al requerir el procesamiento de una transacción determinada	Se permite hacer ciertas transacciones a unos usuarios que otros no pueden hacer dependiendo del tipo de usuario y del Grupo. Se restringe el acceso a ciertos programas a ciertos usuarios cómo definición del perfil por usuario, evitando la instalación de programas por parte del usuario.	No se encontraron debilidades significativas	3	4	1	4 Bajo
Limitaciones a los servicios	Comprobar la existencia de controles que se refieren a las restricciones que dependen de medidas establecidas por el administrador o propias de la utilización de una aplicación.	Si existe en la empresa productos de software cuya licencia limite su uso a un número determinado de usuarios. El administrador a establecido limites al uso simultaneo de ciertas aplicaciones.	No se encontraron debilidades significativas	2	4	1	4 Bajo
Modalidad de acceso	Confirmar si se ha establecido el modo en que se permite el acceso al usuario a los recursos del Sistema de Información.	Existe un procedimiento para la asignación de permisos de acceso, se asigna por usuario y aplicación. El administrador es quién otorga estos permisos y se lo hace por perfil y con autorización del jefe inmediato de cada área. Este procedimiento se encuentra debidamente documentado.	No se encontraron debilidades significativas	3	4	1	4 Bajo
Ubicación y Horario	Verificar si la ubicación física o lógica de los datos o de la personas sirve r para fijar el acceso a determinados recursos del sistema.	El tiempo de conexión no está limitado al horario de trabajo, no se restringe el acceso a determinadas horas del día o días de la semana para mayor control, no se consideran necesarias estas restricciones de acceso.	No se encontraron debilidades significativas	0	No aplica	No aplica	No aplica

Control de acceso interno	Existen los controles para mantener la autenticación del usuario así como la inviolabilidad de la información	Los mecanismos de control de acceso que se utilizan son: Password y Listas de Control de acceso, las que se manejan por sistema integrado, con actualización manual semanalmente. Se usa encriptación para almacenarla. Interfaces de usuarios restringidas, solo ven lo que les está permitido, con la vista de menús. Encriptación, se encriptan los passwords y las cuentas de usuario. Protección de puertos.	No se encontraron debilidades significativas	2	4	1	4 Bajo
Control de acceso externo	Identificar la existencia de controles a os dispositivos que permiten la comunicación de la red interna con la red externa, y de las políticas establecidas para el efecto.	No existe acceso externo a los datos, desde internet o desde módem. Control de acceso para limitar lo que se ve, lee, borra, modifica, etc. Firmas digitales Copias de seguridad de información pública en otro lado, no en la misma máquina Se prohíbe el acceso público a bases de datos vivas Se verifica que los programas y la información pública no tenga virus Usan alguna forma de acceso remoto para cambiar las configuración del sistema	No se encontraron debilidades significativas	2	4	1	4 Bajo
Administración de Personal	Existen procedimientos para la Administración del Personal y Usuarios.	Se tiene una máxima separación de funciones, se otorga el mínimo permiso de acceso requerido para cada puesto, se considera los requerimientos de experiencia y conocimiento para cada puesto. La empresa no tiene establecido un procedimiento de capacitación continua para el personal. El personal es consciente de la importancia de la información como recurso valioso para la empresa.	La empresa no ha establecido un procedimiento de capacitación continua para el personal.	2	3	3	9 Moderado

Fuente: Muñoz, A. (2014).

Analizando la tabla anterior, se puede determinar que las 15 actividades del componente Seguridad Lógica se distribuyen de la siguiente forma:

Tabla 30.

Distribución niveles de madurez Seguridad Lógica		
Nivel	**Número Actividades**	**Porcentaje**
0	1	6.7
1	0	0
2	8	53.3
3	4	26.7
4	2	23.3
5	0	0

Fuente: Muñoz, A. (2014)

Por lo que el componente Seguridad Lógica se encuentra en el Nivel de Madurez 2 de Cobit 4.1.(**Repetible:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.)

En la evaluación de riesgos, de las 15 actividades del componente Seguridad Lógica se clasifican:

Tabla 31.

Distribución de riesgos Seguridad Lógica		
Nivel	**Número Actividades**	**Porcentaje**
ALTO	0	0
MEDIO	2	14.3
BAJO	13	85.7

Fuente: Muñoz, A. (2014)

Es decir 2 actividades requieren de acciones correctivas mediatas, 13 de acciones correctivas eventuales.

Tabla 32.

Análisis Seguridad de la Red.

Elemento	Actividad	Respuesta	Debilidad	Nivel de Madurez	Impacto	Probabilidad	Calificación Riesgo
Topología de Red	Determinar si existe documentación sobre la topología de red utilizada en la empresa.	Existe un gráfico topológico desactualizado Componentes de la red: 60 Pcs distribuidas en la empresa. 1 servidor de archivos. 1 servidor de internet fibra óptica 1 servidor de internet satelital. Descripción de la red: Enlaces radiales o satelitales Fibra óptica UTP en conexiones internas Switches	Diagrama de topología de la red desactualizado, debido a la falta de tiempo y de personal que se dedique a la documentación.	2	3	3	9 Moderado

Conexiones Remotas	Existen conexiones remotas y estas están configuradas de tal manera que garanticen la seguridad de la información.	Al contar con un sistema integrado la empresa no necesita tener oficinas ni sucursales en otras ciudades. Todos los procesos desde la recepción del productos se controlan en línea, ingresando los datos desde las Pcs de producción mediante el ingreso de códigos de barras, lo que permite en un momento dado rastrear una caja del producto desde su origen (camaronera) hasta el lugar de comercialización (en cualquier parte del mundo), este es el sistema de trazabilidad que la empresa ofrece a sus clientes.	No se detectaron debilidades significativas	4	2	2	4 Bajo
Configuración de la red.	Comprobar la correcta configuración de la red, correo electrónico, periféricos, backups.	Los datos van encriptados y pasan por el firewall, existen controles de acceso adecuados a los servidores conectados a internet. No se comparte los discos de las PCs en la red; cada usuario tiene su carpeta con información referente a su puesto de trabajo, no se puede ver las carpetas de mails de los compañeros de trabajo, En cuanto a la fiabilidad existen medios de transmisión de datos alternativo mediante la implementación de switchs extras, se realizan backups continuamente, si no funciona ADSL existe una redundancia de acceso a internet ya que se cuenta con dos servidores de internet, uno para la red con fibra óptica y otra conexión satelital.	No se cuenta con un respaldo en caso de la caída del servidor y de pérdida de información.	2	4	4	16 Alto
		A nivel de puertos se deshabilitaron todos los puertos no necesarios, además se hacen pruebas de los puertos a nivel de servidores, así como del firewall mediante software. Se realizan pruebas periódicas de hackeo utilizando MTEXPLOIT y WARESHARK, además los puertos se prueban con un escaneador. Todos los días se hace chequeo de la red y sus permisos, donde se controla acceso al recurso, cambio de la clave, uso de la clave, estos procedimientos no se documentan.	Si bien se hacen chequeos periódicos de la red, la ejecución de estos y sus resultados no se documentan, se limita a un informe de resultados enviados a través del correo.	2	3	3	9 Moderado

		No existe documentación actualizada de la topología de la red, existen manuales, licencias de software, un documento no actualizado en relación a los planes de contingencia, seguridad. Existe una documentación con la configuración de la red y de las Pcs que incluye números IP, placas de red, etc.	No se detectaron debilidades significativas	2	3	3	9 Moderado
Correo Electrónico	Revisar si existen procedimientos que permitan garantizar la seguridad del servidor de correo.	En el servidor el correo se administra con WebMin, el encargado de su configuración es el administrador. Se chequea que la configuración sea eficiente cuando se da de alta una cuenta o pasando un día. La herramienta con la que los usuarios leen sus mail internamente es OUTLOCK y externamente AQUARREMAIL, lo realizan desde sus PCs. En estas herramientas se encuentra habilitada la vista previa, confirmación de lectura, chequeo de virus en correo entrante y saliente, controles Activex y Scripts, cada usuario tiene su propia cuenta de spam y control para ciertos tipo de archivos	No se detectaron debilidades significativas	2	2	2	4 Bajo
		El servidor automáticamente baja los mails de toda la empresa a sus discos y los reparte a sus destinos, los mails no se borra del servidor. No existen mecanismos de filtrado dentro del encabezado o cuerpo del mensaje para evitar virus o correos no deseados.	No se detectaron debilidades significativas	2	2	2	4 Bajo
		En cuanto al espacio en disco se asigna espacio a cada usuario y a cada cuenta de mail, la cantidad varía de acuerdo al perfil y grupo. Nunca ha sucedido que se llegue al límite de espacio en disco asignado.	No se detectaron debilidades significativas	3	2	2	4 Bajo
		Solo algunos empleados tienen direcciones de mail, esto depende del perfil del empleado, con el mismo mail interno se tiene acceso al mail externo. El mail interno va directamente al servidor de correos, se monitorea esporádicamente para controla que los usuarios no usan el mail para fines personales. Además se controlan los Spams en estas direcciones.	No se detectaron debilidades significativas	3	2	2	4 Bajo

		El correo basura es detectado por el servidor de email, el mismo es enviado a una carpeta temporal para su posterior eliminación.	No se detectaron debilidades significativas	3	2	2	4 Bajo
		Solo personal autorizado puede hacer uso del Chat para esto se usa MSN, internamente se lo realiza con LANMESSENGER, se permite bajar archivos solo internamente con LANMESSENGER, cuando se necesita usar programas de file sharing se utiliza FTP seguro	No se detectaron debilidades significativas	3	2	2	4 Bajo
		Por política de la empresa se prohíbe el envío de archivos u otros documentos confidenciales vía mail. Se utiliza TOKEN para las transacciones estos se usan para mensajes externos, la clave es privada sin embargo la utilizan las secretarias para enviar mensajes a nombre de sus jefes.	No se detectaron debilidades significativas	2	2	2	4 Bajo
Control de Virus	Se ha implementado un procedimiento efectivo para la detección y control de virus	La empresa cuenta con paquetes de software anti virus, firewalls, sistemas de detección de intrusos. Existen procedimientos que se deben seguir para cuando ocurra una infección por virus, la misma que no se ha presentado. Para la detección de virus se tiene instalado MAILSCANNER, en los servidores.	No se detectaron debilidades significativas	2	3	3	9 Moderado
		Todo el trabajo de detección y manejo de los mail con virus lo realiza la herramienta, la misma que fue configurada por el administrador. En las PCs se encuentra habilitado sólo los procesos que el usuario utiliza para su trabajo, inclusive está deshabilitada la unidad de disco C. En cuanto a los correos se cuenta con buenas protecciones para evitar el ingreso de virus por este medio.	No se detectaron debilidades significativas	3	3	2	6 Moderado

		La empresa cuenta con el antivirus MAILSCANNER en el servidor de internet, el mismo que se ejecuta continuamente y controla el correo entrante y saliente, en el servidor como en las Pcs se realiza el respaldo mediante una imagen de disco. Tanto los servidores como las PCs tiene instalado el antivirus. El escaneo en busca de archivos infectados por virus se lo realiza a diario automáticamente, además el firewall y el antivirus están relacionados y son compatibles entre sí.	No se detectaron debilidades significativas	3	3	2	6 Moderado
Muros de Fuego (Fire Walls)	Determinar la correcta configuración del Fire Wall para garantizar la seguridad.	El firewall que se usa es el IPT que se encuentra en el servidor de internet, es del tipo gateway de filtrado de paquetes (packet filtering gateways), utiliza la política de configuración se especifica solo lo que está permitido y se prohíbe todo lo demás. Está configurado para discriminar entre tres clases de paquetes: paquetes entrantes a la red paquetes salientes de la red paquetes en tránsito	No se detectaron debilidades significativas	3	3	1	3 Bajo
		Tiene habilitados los servicios HTTP, SCH, BUFTPD y deshabilitados todos los demás, soporta autenticación, incluye las direcciones NAT en la autenticación, usa password. Incluye registro de intentos no autorizados de ingreso ,genera logs, provee reportes, no tiene alarmas. Se encuentran deshabilitados completamente los servicios o protocolos: SUID, RLOGIN, RSH, REXEC, SU, NetStar, GOPHER, TFTP, Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY.	No se detectaron debilidades significativas	3	3	2	6 Moderado
Control de Ataques a la red	Comprobar si se han implementado procesos que permitan la protección contra ataques a la red.	La empresa no dispone de herramientas para prevenir los ataques de red, debido a que no se ha presentado ningún ataque hasta el momento.	No se detectaron debilidades significativas	1	4	1	4 Bajo
		No existen zonas desmilitarizadas debido al costo que esto implica y porque no hay datos publicados on line desde el interior de la empresa	No se detectaron debilidades significativas	1	4	1	4 Bajo

	No existe ninguna herramienta anti-spoofing. No se configura el acceso externo para que el firewall explícitamente externa que posea una dirección en el interior de la red externa.	No se detectaron debilidades significativas	1	4	1	4 Bajo
	El archivo de los passwords del sistema se almacena en el directorio /etc/passwd. Este archivo está en texto plano y puede ser accesible ya que está en texto plano.	No se detectaron debilidades significativas	1	4	1	4 Bajo

Fuente: Muñoz, A. (2014).

Analizando la tabla anterior, se puede determinar que las 20 actividades del componente Seguridad de la Red se distribuyen de la siguiente forma:

Tabla 33.

Distribución niveles de madurez Seguridad de la Red		
Nivel	**Número Actividades**	**Porcentaje**
0	0	0
1	4	20
2	7	35
3	8	40
4	1	5
5	0	0

Fuente: Muñoz, A. (2014)

Por lo que el componente Seguridad de la Red se encuentra en el Nivel de Madurez 3 de Cobit 4.1.(**Definido:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.)

En la evaluación de riesgos, de las 20 actividades del componente Seguridad de la Red se clasifican:

Tabla 34.

Distribución de riesgos Seguridad de la Red		
Nivel	**Número Actividades**	**Porcentaje**
ALTO	1	5
MEDIO	7	35
BAJO	13	65

Fuente: Muñoz, A. (2014)

En decir 1 actividades requieren de acciones correctivas inmediatas, 7 de acciones correctivas mediatas y 13 de acciones correctivas eventuales.

Tabla 35.

Análisis Seguridad de las Aplicaciones.

Elemento	Actividad	Respuesta	Debilidad	Nivel de Madurez	Impacto	Probabilidad	Calificación Riesgo
Software	Analizar si el software está actualizado, el software desarrollado se encuentre de acuerdo a la política de la empresa.	Para elegir los sistemas operativos y programas usados en la empresa se considero: los requerimientos funcionales, de compatibilidad, de desempeño, de interoperabilidad, fiabilidad, facilidad de uso, costo de mantenimiento. También se consideraron aspectos de seguridad como: identificación y autenticación, control de acceso, incorruptibilidad, fiabilidad, seguridad de las transmisiones, backup de datos, entre otros. Una vez analizados estos aspectos se tomó la decisión de cual sistema operativo y programas se instalaran	No se detectaron debilidades significativas.	2	3	3	9 Moderado
		Los cambios a los archivos del sistema o a las bases de datos se deben realizar como parte de la programación del CPD, existen registros de datos de salida. Solamente están autorizadas tres laptops dentro de la empresa y son de uso exclusivo del gerente, auditora y jefe de sistemas.	En las bases de datos no se controla los siguientes puntos: Tiempo y duración de los usuarios en el sistema. Número de intentos fallidos de conexión a la base de datos. Ocurrencias de bloqueo (deadlock) con la base de datos. Estadísticas de entrada salida para cada usuario.	2	3	4	12 Moderado
		Está asegurada la exactitud de los datos, existe un control de cambios para el desarrollo de aplicaciones. Se realiza el control de los datos de entrada, se verifica la existencia de los archivos antes de su ejecución. Se revisa la consistencia de los datos de salida de las aplicaciones.	No se detectaron debilidades significativas.	3	3	2	6 Moderado

Bases de Datos	Verificar la integridad y consistencia de los datos y la ausencia de redundancias.	Los archivos de las Bases de Datos cuentan con control de acceso, realizando los siguientes controles: número de conexiones a bases de datos, generación de nuevos objetos de bases de datos, modificación de bases de datos. De igual manera se hace chequeos regulares de la seguridad de la base de datos, el acceso a los archivos de la BD los sistemas operativos y a las tablas del sistema además del administrador lo tienen dos funcionarios del departamento de sistemas.	No se detectaron debilidades significativas.	3	4	1	4 Bajo
		No existen usuarios que tengan los mismos permisos que el administrador, la base de datos tiene suficientes recursos libres para trabajar, los registros de las bases de datos cuando un usuario los elimina se marcan como borrados para su posterior eliminación.	No se detectaron debilidades significativas.	3	4	1	4 Bajo
Aplicaciones en Pc's	Determinar la existencia de normas que se han de aplicarse para la configuración y uso de Pc's.	Todas las PCs de la empresa tienen instalado los mismos programas con las mismas versiones, los mismos que fueron autorizados por el departamento de sistemas, así mismo todas las PCs tienen una configuración estándar.	No se detectaron debilidades significativas.	3	3	1	3 Bajo
		Existe un procedimiento para instalar aplicaciones en las máquinas de los usuarios, así como para la instalación o actualización de parches en las aplicaciones, estos procesos son realizados exclusivamente por el asistente de sistemas y es documentado mediante bitácoras. De igual forma existe un procedimiento para encontrar programas que no deberían estar en las máquinas, para los cual se utiliza la herramienta BELARC. Los usuarios tienen acceso al internet de acuerdo a perfiles, es prohibido instalar software y aplicaciones bajadas de la web como versiones de prueba o demo	No se han establecido procedimientos que eviten ingresar y registrar software no autorizado por parte de los empleados.	2	4	3	12 Moderado

Ciclo de Vida	La seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.	La empresa cuenta con aplicaciones propias desarrolladas por el departamento de sistemas para cada área de empresa, se aplica la metodología de desarrollo conocida como YOURDON, que consta de las siguientes fases: análisis, desarrollo, pruebas e implementación; se implementan validaciones a nivel de objetos.	No se detectaron debilidades significativas.	3	3	1	3 Bajo
		Las necesidades de las aplicaciones a desarrollar se expresan a través de reuniones de trabajo con el personal del área que solicita la aplicación, estas necesidades se plasman en un documento. Antes de iniciar con el desarrollo se realiza un análisis de riesgos, en caso de trabajar con terceros esta debe sujetarse a la reglamentación establecida para el efecto.	No se detectaron debilidades significativas.	4	3	1	3 Bajo
		Las aplicaciones se implementan en POWERBUILDER, durante la implementación se realiza validación de datos y pruebas de acceso a través de menús. Para las pruebas se generan planes de pruebas, se realizan pruebas por módulos, para lo cual se generan escenarios, no se documentan las pruebas y sus resultados en papel, solo a través de informes por correo.	No se detectaron debilidades significativas.	2	4	1	4 Bajo
		En la instalación y mantenimiento no se usa ninguna metodología específica, simplemente queda a criterio de la persona de sistemas designada para el efecto. Se documenta los sistemas desarrollados.	No se documentan los cambios de emergencia al realizar el mantenimiento de las aplicaciones. No se obtiene un backup de la configuración de los sistemas antes de hacer un cambio.	2	3	3	9 Moderado
		En el caso de que se compre el sistema primero se establece la funcionalidad, la disponibilidad del proveedor y un análisis costo beneficio, al comprar el sistema se exige la documentación del mismo.	No se detectaron debilidades significativas.	3	3	1	3 Bajo

Fuente: Muñoz, A. (2014).

Analizando la tabla anterior, se puede determinar que las 12 actividades del componente Seguridad de las Aplicaciones se distribuyen de la siguiente forma:

Tabla 36.

Distribución niveles de madurez Seguridad de las Aplicaciones		
Nivel	**Número Actividades**	**Porcentaje**
0	0	0
1	0	0
2	5	41.7
3	6	50
4	1	8.33
5	0	0

Fuente: Muñoz, A. (2014)

Por lo que el componente Seguridad de las Aplicaciones se encuentra en el Nivel de Madurez 3 de Cobit 4.1 (**Definido:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.)

En la evaluación de riesgos, de las 12 actividades del componente Seguridad de las Aplicaciones se clasifican:

Tabla 37.

Distribución de riesgos Seguridad de las Aplicaciones		
Nivel	**Número Actividades**	**Porcentaje**
ALTO	0	0
MEDIO	5	41.7
BAJO	7	58.3

Fuente: Muñoz, A. (2014)

Es decir 5 actividades requieren acciones correctivas mediatas y 7 actividades acciones correctivas eventuales.

Tabla 38.

Análisis Seguridad Administración CPD.							
Elemento	**Actividad**	**Respuesta**	**Debilidad**	**Nivel de Madurez**	**Impacto**	**Probabilidad**	**Calificación Riesgo**
Administración del CPD.	Evaluar la organización y administración del departamento de sistemas, asignación de tareas, procedimientos y responsabilidades del personal, con el objetivo de brindar un ambiente	Las responsabilidades puntuales son asignadas a cada empleado, estas responsabilidades para las funciones de TI son realizadas por el jefe de sistemas. El encargado de la seguridad y de las políticas de seguridad y administración es el jefe de sistemas. Es quién realiza la planificación y asigna las tareas a los empleados del CPD.	No se encontraron debilidades significativas	2	3	2	6 Moderado

	adecuado y seguro para brindar un servicio de calidad a la institución.	No se ha implementado la mesa de reporte de incidentes, no existe un buzón de sugerencias.	No se ha definido claramente a donde tienen que acudir los usuarios a reportar incidentes de seguridad y solicitar asesoramiento de las acciones a seguir con la finalidad de reducir o eliminar estos sucesos.	0	3	5	15 Moderado
		Existe una planificación de las actividades que desarrollará el CPD: procesos a realizar, controles, mecanismos de registro, mecanismos de distribución de información	No se encontraron debilidades significativas	3	3	4	12 Moderado
		Los backups se realizan diariamente, es un proceso que se lo realiza automáticamente mediante programación Bash Shelly tareas programadas el mismo que está a cargo del administrador de sistemas.	No se encontraron debilidades significativas	2	4	4	16 Alto
Capacitación	Comprobar la aplicación del Plan de Capacitación para los funcionarios del CPD.	Las nuevas normas de seguridad se dan a conocer a través de charlas y reuniones con los empleados, lo que ha dado buen resultado hasta el momento por cuanto todos conocen lo que hay que hacer para garantizar las seguridad. Cuando ingresa un empleado nuevo a la empresa se lo capacita en el uso del sistema.	La empresa no ha establecido un procedimiento de capacitación continua para el personal.	2	4	4	16 Alto

Backups	Verificar la existencia de un procedimiento formal y documentado para la obtención de backups del sistema.	Estos backups son normales, se almacenan en Disco Duro y CDs, cada seis meses se graba la información en CDs y se entregan tres copias: una a Gerencia, una a Auditoría Interna y una al Jefe de Sistemas. Los backups se almacenan dentro y fuera de la empresa en lugares seguros, en la documentación escrita de los backups solo se anota la fecha de realización. La empresa no posee información en la Web, solo cuenta con páginas estáticas de las cuales si existe respaldo. No se hace ningún backup de los logs del sistema, solo se los almacena y depura periódicamente.	No se encontraron debilidades significativas	2	4	3	12 Moderado
Documentación	Confirmar que todos los procedimientos y acciones del CPD estén debidamente documentados.	En el centro de procesamiento de datos existe documentación sobre: actividades que se desarrollan normalmente , los procesos a realizar, los controles que se efectúan, las relaciones con otras áreas, mecanismos de distribución de la información.	Existe una gran deficiencia en cuanto a la documentación de las actividades principales y secundarias del Centro de Procesamiento de Datos, debido a que no se cuenta con el personal para que se dedique a esta..	2	3	4	12 Moderado
		Documentación detallada sobre el equipamiento. distribución física (PCs, equipos y puestos de trabajo), inventario de hardware y software, número de serie del hardware, número de licencia de software, inventario de insumo, ubicación de nodos. Se cuenta con una documentación del Plan de contingencia, Plan de seguridad, manuales de procedimientos del CPD, manuales de usuario por procesos, manuales del sistema, manuales de operación, manuales de seguridad.	No se encontraron debilidades significativas	4	3	3	9 Moderado

	El responsable de administrar las emergencias y de implantar las políticas de seguridad de la información es el Jefe de Sistemas, el mismo que tiene todos los privilegios, es quien asigna los permisos a los diferentes roles, es quien está encargado de reportar a los ejecutivos de la empresa sobre la administración de seguridad. Se realizan informes a través del correo interno, existe en los ejecutivos de la empresa la conciencia de la importancia de la seguridad.	No se encontraron debilidades significativas	2	4	4	16 Alto

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que las 9 actividades del componente Administración del CPD se distribuyen de la siguiente forma:

Tabla 39.

Distribución niveles de madurez Seguridad Administración CPD		
Nivel	**Número Actividades**	**Porcentaje**
0	0	0
1	1	11.1
2	6	66.7
3	1	11.1
4	1	11.1
5	0	0

Fuente: Muñoz, A. (2014)

Por lo que el componente Administración del CPD se encuentra en el Nivel de Madurez 2 de Cobit 4.1. (**Repetible:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.)

En la evaluación de riesgos, de las 9 actividades del componente Administración del CPD se clasifican:

Tabla 40.

Distribución de riesgos Administración CPD		
Nivel	**Número Actividades**	**Porcentaje**
ALTO	3	33.3
MEDIO	6	66.7
BAJO	0	0

Fuente: Muñoz, A. (2014)

Es decir 3 actividades requieren acciones correctivas inmediatas y 6 actividades acciones correctivas mediatas.

Tabla 41.

Evaluación Plan de seguridad.

Elemento	Actividad	Respuesta	Debilidad	Nivel de Madurez	Impacto	Probabilidad	Calificación Riesgo
Administración de Incidentes	Comprobar la documentación sobre la forma de hacer frente a los diferentes errores que pueden devastar la infraestructura de TI (Tales como la pérdida completa de los servidores, los datos, routers, puentes, comunicación, enlaces, etc.	Existe un Plan de Seguridad con las normas y controles establecidos. Todas estas normas y controles no se encuentran documentados y condensados de manera adecuada en un plan de seguridad. Existe un plan de contingencias desarrollado por el administrador de sistemas.	No se detectaron debilidades significativas	3	4	4	16 Alto
		No se documenta no existe un documento que detalle: Objetivo Modo de ejecución Tiempo de duración Costes estimados Recursos Evento que dispara el plan Personas encargadas de ejecutar el plan	Existe un Plan de Seguridad pero en el mismo no se incluye un Plan de Recuperación de Desastres, no se definen las responsabilidades y funciones de las personas en el plan de contingencia, no hay ningún mecanismo de reportes o historial para el manejo de incidentes, no se documenta el plan de contingencias y no se hacen pruebas del plan.	2	4	4	16 Alto
Backups de equipos	Comprobar la existencia de un centro de respaldo con el equipamiento de hardware y software que permita minimizar el tiempo de recuperación de las actividades del CPD.	No se cuenta con un centro de procesamiento de datos alternativo, ya que de acuerdo a información del administrador no se justifica esta inversión; los servidores se encuentran en una sola habitación.	No se cuenta con equipos de respaldo que puedan en caso de una emergencia o daño de los equipos principales mantener en funcionamiento los sistemas de los que depende la empresa.	0	5	3	15 Moderado

Recuperación de desastres	Verificar la existencia de un Plan detallado de Recuperación de Desastres	No existe un Plan de Recuperación de desastres establecido formalmente, solo se cuenta con las normas y controles establecidos para los diferentes aspectos anteriormente analizados como seguridad física, seguridad lógica, de las aplicaciones, de la red, administración. Todas estas normas y controles no se encuentran documentados y condensados de manera adecuada en un plan de seguridad.	no se incluye un Plan de Recuperación de Desastres, no se definen las responsabilidades y funciones de las personas en el plan de contingencia, no hay ningún mecanismo de reportes o historial para el manejo de incidentes, no se documenta el plan de contingencias y no se hacen pruebas del plan	1	5	3	15 Moderado
		Existe un plan de contingencias desarrollado por el administrador de sistemas, el mismo que se lo desarrollo previo un análisis de riesgo, se tomó en cuenta no solo al área de sistemas sino a todas las áreas de la empresa, esto considerando que todos los sistemas están completamente integrados.	No existe en la empresa un plan de Recuperación del Centro de Procesamiento de Datos.	3	5	3	15 Moderado
		No se cuenta con un Plan de Respuesta a incidentes, la respuesta a incidentes de seguridad se la realiza a criterio del administrador de sistemas	No se cuenta con un documento formal para la evaluación de daños, sistemas afectados, equipos operativos, tiempo de recuperación.	1	5	3	15 Moderado

Fuente: Muñoz, A. (2014)

Analizando la tabla anterior, se puede determinar que las 6 actividades del componente Análisis Plan de Seguridad se distribuyen de la siguiente forma:

Tabla 42.

Distribución niveles de madurez Plan de Seguridad		
NIVEL	**NÚMERO ACTIVIDADES**	**PORCENTAJE**
0	1	16.7
1	2	33.3
2	1	16.7
3	2	33.3
4	0	0
5	0	0

Fuente: Muñoz, A. (2014)

Por lo que el componente Análisis Plan de Seguridad en promedio se encuentra en el Nivel de Madurez 2 de Cobit 4.1 (**Repetible:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay

entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.)

En la evaluación de riesgos, de las 6 actividades del componente Análisis Plan de Seguridad se clasifican:

Tabla 43.

Distribución de riesgos Plan de Seguridad		
Nivel	**Número Actividades**	**Porcentaje**
ALTO	2	33.3
MEDIO	4	66.7
BAJO	0	0

Fuente: Muñoz, A. (2014)

Es decir 2 actividades requieren acciones correctivas inmediatas y 4 actividades acciones correctivas mediatas.

Resumen Niveles de Madurez y Riesgo por Componentes.

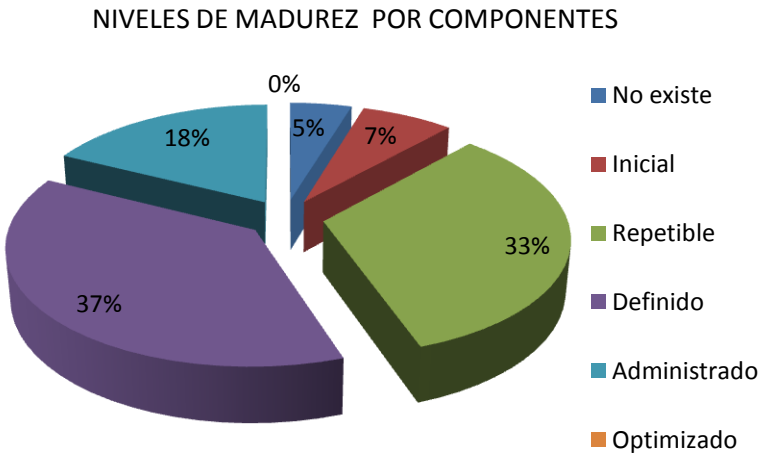


Figura 11: Distribución Niveles de Madurez por componentes
Fuente: Muñoz, A. (2014).

Observando el gráfico se puede determinar que la seguridad en el centro de procesamiento de datos se encuentra distribuida entre los niveles de madurez 2 Repetible y 3 Definido, esto quiere decir que se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea.

No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

Algunos procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

El 18% se encuentra en el nivel 4 Administrado; es decir se puede monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

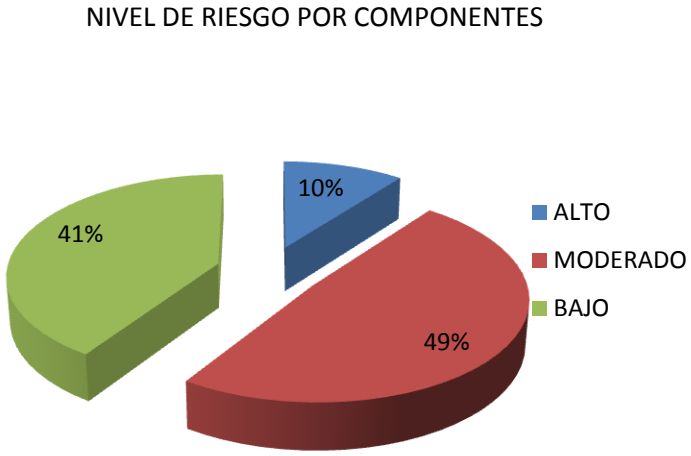


Figura 12: Distribución Niveles de riesgo por componentes
Fuente: Muñoz, A. (2014).

En lo referente al nivel de riesgo estos se han clasificado en un 49% como de riesgo moderado, los mismos que necesitan tomar medidas a mediano plazo para mitigar su impacto para la empresa. Un 41% está clasificado como de riesgo bajo, es decir estos no representan mayor impacto para la empresa, pero se debe monitorear y actualizar las medidas de prevención implantadas para mantenerlos es ese nivel.

Solo un 10% de las actividades se han clasificado como de riesgo alto, es decir actividades que tienen que ser atendidas de manera urgente ya que en caso de suceder presentan un impacto importante para la empresa comprometiendo su funcionamiento.

Capítulo V.
DESARROLLO APLICACIÓN WEB

5.1. Descripción Global del Producto.

5.1.1. Perspectiva del Producto.

El aplicativo a desarrollar es un sistema que permitirá al auditor registrar las actividades, procesos y resultados de la auditoría de seguridad de la información de manera fácil, permitiendo la realización de consultas por componentes, elementos, preguntas, respuestas, estándares, debilidades, efectos y recomendaciones.

5.1.2. Resumen de características.

A continuación se mostrará un listado con los beneficios que se obtendrá a partir del producto:

Tabla 44.

Características del producto	
Beneficio.	**Características que lo apoyan**
Registro de encuestas para auditoria.	Registro de Preguntas por componentes
Documentar la información obtenida de la auditoría.	Registro de Respuestas
Consultar el estándar utilizado.	Gestión Estándar
Conocimiento de las debilidades, efectos y recomendaciones	Consultas por componentes

Fuente: Muñoz, A. (2014)

5.2. Descripción del sistema a Desarrollarse.

5.2.1. Gestión Elementos.

Se utiliza para actualizar la tabla elementos de la auditoría. Permite introducir la información de los elementos de cada componente que serán objeto de revisión durante la auditoría. También se utiliza para revisar los elementos que ya se han realizado.

5.2.2. Gestión Preguntas.

Se utiliza para actualizar la tabla Preguntas que contiene información sobre los cuestionarios aplicados en la auditoría. Permite introducir las preguntas que se realizarán para recabar información de los elementos a auditar. Por otra parte permite revisar las preguntas ya ingresadas.

5.2.3. Gestión Respuestas.

Se utiliza para actualizar la tabla Respuestas que contiene información sobre las respuestas a los cuestionarios aplicados en la auditoría. Permite introducir las respuestas, debilidades,

efectos y recomendaciones de cada elemento auditado. Por otra parte permite revisar las respuestas y el análisis de los registros ya ingresados.

5.2.4. Gestión Consultas.

Se utiliza para consultar la información de la auditoría, referente a elementos auditados; preguntas realizadas en las entrevistas por cada elemento, las respuestas a los cuestionarios aplicados en la auditoría y las debilidades encontradas, efectos que estas ocasionan y las recomendaciones para mitigar los efectos de cada debilidad detectada.

5.3. Restricciones.

Las restricciones del proyecto se presentan a continuación:

- El sistema web contendrá la interfaz necesaria y útil para presentar información sobre los componentes y elementos de la auditoría; ingresar información y permitir la consulta de las debilidades, efectos y recomendaciones.
- La aplicación no se integrará con ningún otro sistema.
- El sistema web no podrá presentar documentación de respaldo ya que la empresa no autorizó el escaneo de los mismos por considerarlos de uso exclusivo de la empresa.
- El sistema permitirá el acceso al público, con la finalidad de servir como elemento de consulta de la realización de una auditoría de seguridad de la información.
- El acceso al área de administración se lo realizará con usuario y clave, teniendo el auditor el acceso exclusivo para ingresar la información de la auditoría en todas las tablas.

5.4. Precedencia y Prioridad.

El módulo de administrador se considera el más importante, debido a que en este se ingresa y actualiza la información necesaria para la realización y administración de la auditoría.

El módulo de consultas es el segundo en importancia, ya que este permite a los usuarios finales, consultar toda la información referente a una auditoría de seguridad de la información.

5.5. Otros Requisitos del Producto.

5.5.1. Requisitos aplicables a todo el proyecto:

- Los sistemas y los subsistemas deben ejecutarse dentro del cronograma planificado.

- El desarrollo del sistema y los subsistemas se realizarán en plataformas de software libre.
- El proyecto total, deberá cumplir con todos los requerimientos funcionales establecidos.
- La entrega total del proyecto debe ser en funcionamiento completo para su inmediata utilización.

5.5.2. Requisitos del Sistema.

Los requisitos de los sistemas, se presentan a continuación:

- El sistema de administración se construirá sobre la plataforma PHP y MYSQL.
- El sistema de consultas, se construirá sobre la plataforma PHP y MYSQL.

5.5.3. Atributos y Características del Producto de Software.

- Interfaz amigable con el usuario
- Facilidad de uso
- Características de seguridad
- Fiabilidad requerida de los sistemas
- Tamaño correcto de base de datos

5.6. Descripción del Producto.

5.6.1. Perspectiva del Producto.

La aplicación web se diseñará de tal manera que permita contar en una base de datos con la información recolectada durante el proceso de auditoría, así como el estándar que servirá como base para el análisis y las debilidades encontradas, los efectos que estas debilidades provocan en la seguridad; con estos datos se definirán las recomendaciones necesarias para minimizar o eliminar estas debilidades.

5.6.2. Características de los usuarios.

Tabla 45.

Características de los usuarios	
Tipo de usuario	Gerente General.
Formación	Conocimientos sólidos de administración de empresas.
Habilidades	Manejo de computadoras y toma de decisiones.
Actividades	Generar, analizar y tomar decisiones en función de las recomendaciones que se presentan en el sistema.
Tipo de usuario	Jefe de Sistemas.
Formación	Conocimientos sólidos en ingeniería de sistemas y redes.
Habilidades	Manejo y Administración del CPD y toma de decisiones.
Actividades	Analizar y tomar decisiones en función de las recomendaciones que

	se presentan en el sistema.
Tipo de usuario	Administrador de la Aplicación.
Formación	Conocimientos de Sistemas y Auditoría.
Habilidades	Gestión de auditoría, manejo de computadores.
Actividades	Generar y cargar los datos necesarios para la auditoría.
Tipo de usuario	Usuario General.
Formación	Estudiante de auditoría o sistemas.
Habilidades	Manejo de computadoras, internet.
Actividades	Consultar las actividades que se realizan en una auditoría.

Fuente: Muñoz, A. (2014)

5.6.3. Restricciones.

La aplicación será desarrollada en PHP, bajo el entorno de desarrollo DREAMWEAVER, el motor de base de datos será MYSQL. La metodología de desarrollo del aplicativo se basará en el Proceso Unificado de Rational (RUP). Para la documentación en UML se utilizará StarUML.

Por pedido de los ejecutivos de la empresa auditada, en este trabajo no se presentará ningún documento de respaldo de la auditoría, la razón expuesta es por motivos de confidencialidad y seguridad de la empresa.

5.6.4. Suposiciones y dependencias.

Se debe desarrollar la aplicación Web para recoger información a analizar y determinar su cumplimiento basados en el estándar Cobit las debilidades y efectos para cada componente de la auditoría, una vez analizada la información se procederá a realizar las recomendaciones que permitan minimizar o suprimir estas debilidades.

5.6.5. Requisitos específicos.

- Descripción del Requisito Funcional
- Permitir la autentificación del administrador.
- Permitir el acceso a cualquier usuario interesado en consultar el proceso de auditoría.
- Permitir la gestión (crear, modificar y eliminar) información referente a la auditoría.
- Permitir la consulta de información de la auditoría por componentes.

5.6.6. Requisitos comunes de los interfaces.

Interfaces de usuario.

Las interfaces de usuario están relacionadas con las pantallas, ventanas (formularios) que debe manipular el usuario para realizar una operación determinada. El usuario la realizará mediante el teclado y el mouse del computador.

Las interfaces de usuario ayudaran al usuario trabajar en un ambiente adecuado, además ejecutar las funcionalidades de los sistemas correctamente, por lo que dichas interfaces incluirán:

- Botones
- Menús
- Submenú
- Listas

Interfaces de hardware.

- La pantalla del monitor.- La aplicación se deberá ajustar a cualquier tamaño de pantalla de monitor de PC.
- Mouse.- El sistema deberá interactuar con el movimiento del ratón y los botones del mouse.
- Teclado.- El sistema deberá interactuar con las pulsaciones del teclado.

Interfaces de software

El sistema tendrá una interfaz amigable con el usuario para el registro y consulta de información.

5.7. Requisitos funcionales.

- El sistema debe permitir el ingreso del usuario y contraseña para realizar las diferentes funciones que tendrá el administrador.

- El sistema de debe permitir al administrador la gestión de la auditoría en todas sus etapas y componentes (ingreso, modificación, consulta y eliminación) de la información.

- El sistema debe permitir la consulta de: preguntas(entrevistas), respuestas(información de la auditoría), estándar aplicado, debilidades, efectos y recomendaciones; por cada componente de la auditoría.

- El sistema debe permitir el acceso a cualquier usuario que desee conocer y consultar el proceso de auditoría de la información.

5.8. Requisitos no Funcionales.

5.8.1. Requisitos de rendimiento.

El sistema será desarrollado de acuerdo a los requerimientos del auditor, el mismo estará operativo las 24 horas del día los 365 días del año.

5.8.2. Seguridad.

La seguridad del sistema para el acceso del administrador se basa en el usuario y contraseña, siendo el administrador el único que puede acceder al modulo de gestión, es decir, solo él puede ingresar y modificar información de las bases de datos.

5.8.3. Fiabilidad.

Es uno de los factores que dará confianza al administrador, ya que los usuarios solo tienen acceso a consultas y no pueden ingresar a modificar las bases de datos.

5.8.4. Disponibilidad.

El sistema será instalado en un servidor web, estando disponible el 100 por ciento del tiempo salvo en los momentos que se encuentre en mantenimiento.

5.8.5. Portabilidad.

Una de las ventajas de utilizar plataformas basadas en SW libre, es que no tendremos que, pagar costos por el uso de plataformas propietarias.

El uso de las plataformas de software libre en que trabajaremos garantiza a los sistemas a desarrollarse lo siguiente:

- Es portable la aplicación por el simple hecho de utilizar el lenguaje y plataforma PHP.
- Es portable al utilizar la base de datos MYSQL, es decir puedo tenerlo en Windows o Linux.
- Soporte y documentación gratuita sobre el manejo y uso de estas plataformas.

5.9. Plan de desarrollo de Software.

5.9.1. Propósito.

El propósito de este documento es proporcionar la información necesaria para controlar y proveer una visión global del enfoque de desarrollo propuesto para la aplicación Web que, permita documentar, dar seguimiento y facilitar la consulta del proceso de esta auditoría.

El desarrollo de este proyecto está basado en la metodología Rational Unified Process (RUP), de acuerdo a las características y necesidades encontradas. En este artefacto de RUP se muestra los roles de los participantes, las actividades a realizarse y los artefactos que serán generados en cada etapa.

5.9.2. Alcance.

El presente documento describe el plan general a ser usado para el desarrollo de la aplicación web para consulta y administración de la auditoría de seguridad de la información.

5.9.3. Resumen.

Después de esta introducción, el resto del documento está organizado, en las siguientes secciones:

- Vista General del Proyecto.- Proporciona una descripción del propósito, alcance y objetivos del proyecto, estableciendo los artefactos que serán producidos y utilizados durante el proyecto.
- Organización del Proyecto.- Describe la estructura organizacional del equipo de desarrollo.
- Gestión del Proceso.- Explica la planificación estimada, define las fases e hitos del proyecto y describe cómo se realizará su seguimiento.
- Planes y Guías de aplicación.- Proporciona una vista global del proceso de desarrollo de software, incluyendo métodos, herramientas y técnicas que serán utilizadas.

5.10. Vista General del Proyecto.

5.10.1. Propósito.

El propósito de la aplicación es proporcionar la información necesaria para la administración de una auditoría de seguridad de la información.

Los usuarios de esta aplicación son:

- El Auditor informático que la utiliza para dar seguimiento al proceso y el análisis de, los datos recopilados.
- El usuario que la utilizará para consultar y entender la manera en que se desarrolla una, auditoría de seguridad de la información.

5.10.2. Alcance.

El aplicativo se basará en el estudio y análisis de la información recolectada en base a los siguientes componentes:

- Seguridad Física.
- Seguridad Lógica.
- Seguridad de la Red.
- Seguridad de las Aplicaciones.
- Administración del CPD.
- Análisis del Plan de Seguridad.

5.10.3. Objetivos.

- Documentar el proceso de auditoría de la seguridad informática de un CPD.
- Permitir a los auditores revisar y actualizar la información de la auditoría.
- Facilitar el análisis de la información recopilada en la auditoría.
- Dar al cliente la facilidad de consultar sobre las debilidades y efectos de estas para la seguridad de la información, así como las recomendaciones que permitan eliminar o minimizar los efectos de las mismas.

5.11. Entregables del proyecto.

A continuación se presenta la lista de artefactos propuestos para el proyecto en base a la metodología RUP:

5.11.1. Inicio:

- Documento de Visión (Ver Anexo 8)
- Especificación de Requerimientos (Ver Anexo 9)

5.11.2. Elaboración:

- Plan de desarrollo de software. (Ver Anexo 10)

5.11.3. Documento de Arquitectura que contiene: (Ver Anexo 11)

- Diagrama de clases.
- Diagrama de objetos.
- Diagrama de secuencia.
- Diagrama de colaboración.
- Diagrama de casos de uso.
- Diagrama de estados.
- Diagrama de actividades.
- Diagrama de componentes.
- Diagrama de despliegue.

5.11.4. Construcción: (Ver Anexo 12)

- Construcción del módulo del administrador.
- Construcción del módulo de consultas.

5.12. Organización del Proyecto.

5.12.1. Participantes en el Proyecto.

El personal del proyecto considerando las fases de Inicio, Elaboración, Construcción y Transición estará formado por los siguientes puestos de trabajo:

Tabla 46.

Participantes Proyecto	
Jefe de Proyecto	Con experiencia en metodología de desarrollo RUP, gerencia de proyectos, notación UML y desarrollo de software.
Analista de Sistemas	Informático con conocimientos de UML, uno de ellos al menos con experiencia en sistemas afines a la línea del proyecto
Programadores	Con experiencia en el entorno de desarrollo del proyecto, con el fin de que los prototipos puedan ser lo más cercanos posibles al producto final.
Ingeniero de Software	Persona que participará realizando labores de gestión de requisitos, gestión de configuración, documentación y diseño de datos. Encargada de las pruebas funcionales del sistema, realizará la labor de Tester.

Fuente: Muñoz, A. (2014)

Cabe indicar que estos roles de trabajo serán asumidos por el desarrollador de esta aplicación.

5.12.2. Roles y Responsabilidades.

A continuación se describen las principales responsabilidades de cada uno de los puestos en el equipo de desarrollo durante las fases de Inicio, Elaboración, Construcción y Transición, de acuerdo con los roles que desempeñan en RUP.

Jefe de Proyecto.

- El jefe de proyecto posee las siguientes responsabilidades:
- Asignar los recursos,
- Gestiona las prioridades,
- Coordina las interacciones con los clientes y usuarios, y
- Mantiene al equipo del proyecto enfocado en los objetivos.

El jefe de proyecto también establece un conjunto de prácticas que aseguran la integridad y calidad de los artefactos del proyecto. Además, el jefe de proyecto se encargará de supervisar el establecimiento de la arquitectura del sistema. Gestión de riesgos, planificación y control del proyecto.

Analista de Sistemas.

- El analista de sistemas posee las siguientes responsabilidades:
- Captura de requerimientos,
- Especificación de requerimientos y
- Validación de requerimientos del proyecto,
- Interactuar con el cliente y los usuarios mediante entrevistas.
- Elaboración del Modelo de Análisis y Diseño.
- Colaboración en la elaboración de las pruebas funcionales y el modelo de datos.

Programador

- El programador posee las siguientes responsabilidades:
- Construcción de prototipos,
- Colaboración en la elaboración de las pruebas funcionales,
- Modelo de datos y
- Validaciones del sistema con el usuario.

Ingeniero de Software

- El ingeniero de software posee las siguientes responsabilidades:
- Gestión de requisitos,

- Gestión de configuración y cambios,
- Elaboración del modelo de datos,
- Preparación de las pruebas funcionales,
- Elaboración de la documentación, y
- Elaborar modelos de implementación y despliegue.

5.13. Planes y Guías de aplicación.

5.13.1. Metodología a utilizar.

Para el desarrollo de la aplicación se utilizará la metodología RUP (Rational Unified Process), ya que es framework de procesos adaptables y con la posibilidad de seleccionar los elementos del proceso más apropiados a cada necesidad.

RUP divide el proyecto en 4 fases: Inicio, Elaboración, Construcción y Transición.

5.13.2. Herramientas.

- MySQL como servidor de base de datos
- Macromedia Dream Weaver 8.0 editor web
- Apache como servidor Web
- StarUML diagramador UML

5.13.3. Formulación:

Realizar una aplicación Web que permita al auditor informático la gestión de los componentes de la auditoria de la seguridad informática de un centro de procesamiento de datos, a los clientes y usuarios en general consultar las preguntas que permitieron obtener la información necesaria para la realización de la auditoria, el estándar internacional aplicado, las debilidades efectos y recomendaciones establecidas al final de la auditoria.

5.13.4. Objetivos:

- Documentar el proceso de auditoría de la seguridad informática de un CPD.
- Permitir a los auditores revisar y actualizar la información de la auditoría.
- Facilitar el análisis de la información recopilada en la auditoría.
- Dar al cliente la facilidad de consultar sobre las debilidades y efectos de estas para la seguridad de la información, así como las recomendaciones que permitan eliminar o minimizar los efectos de estas debilidades.

CAPÍTULO 6.
CONCLUSIONES Y RECOMENDACIONES

1.7. **Introducción.**

Una vez analizada la información en base al estándar internacional, y de acuerdo al objetivo planteado, “Conocer vulnerabilidades en los controles, políticas, planes y procedimientos de Seguridad, a fin de establecer los correctivos que permitan minimizar los efectos de estas y alcanzar los objetivos fundamentales de la Gestión de la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad.”

Se presenta en este capítulo las conclusiones (vulnerabilidades) detectadas y los correctivos (recomendaciones) que deben implementarse para garantizar la confidencialidad, integridad y disponibilidad de la información.

6.1.1. Conclusiones.

Generales:

- Los ejecutivos de la empresa están conscientes de la importancia de la información como recurso estratégico; sin embargo no han implementado las políticas, normas y procedimientos estandarizados, dejando toda la responsabilidad en manos del administrador del CPD.
- En relación al estándar Cobit 4.1. la organización se encuentra en el nivel de madurez 1 **Inicial**: es decir existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
- En lo relacionado al nivel de riesgo luego del análisis realizado se determina que se encuentra en el nivel de **riesgo medio;** esto quiere decir que se deben tomar acciones correctivas a mediano plazo.
- Del análisis realizado por componentes se desprende que el nivel de madurez en que se encuentran los controles de la información es entre **nivel 2 de Cobit Repetible:** lo que quiere decir que en algunos procesos se han desarrollado los acciones hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables. Y otros en el **nivel 3 de Cobit, Definido:** es decir los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos,

y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

- El nivel de riesgo analizado por componentes indica que se encuentra en el nivel de **riesgo medio,** concordando con el resultado del análisis hecho con Cobit.
- La aplicación Web desarrollada cumple con la finalidad para la cual fue desarrollada, es decir documentar y facilitar la administración de los componentes auditados.
- No existe el compromiso firme de los ejecutivos de la empresa en aplicar las recomendaciones de la presente auditoría, manifestando que los cambios se lo harán de acuerdo a las disponibilidades si existieran.

Específicas:

- A pesar de contar con un circuito cerrado de televisión, no existe una cámara enfocada hacia la puerta de acceso al CPD. No existe un control minucioso ya que cualquier persona que se encuentre dentro de la empresa, puede ante un descuido del personal ingresar a él poniendo en peligro los equipos y la información que se encuentran en el mismo.
- El CPD no cuenta con alarmas contra fuego, humo e intrusos. Al no existir una alerta en caso de presencia de fuego, humo o intrusos en el CPD, la acción de mitigación de estos podría no ser oportuna, ocasionando graves daños a los equipos y a la información en ellos almacenadas.
- Como el edificio no fue diseñado específicamente para albergar el Centro de Procesamiento de Datos, no se tomó en consideración las medidas de seguridad para los datos y equipos, el CPD no está ubicado en pisos altos, el piso y el techo no están fabricados con materiales ignífugos. Por encontrarse la empresa casi a nivel del mar (a 500 metros de distancia), cerca al río Coaque, existe la posibilidad aunque remota de una inundación que afectaría gravemente al CPD por encontrarse a nivel del suelo, de igual manera al producirse un incendio los materiales con los que están construidos el piso y techo del CPD permitirían la rápida propagación del fuego, reduciendo considerablemente la posibilidad de una acción de contención oportuna lo que ocasionaría daños graves a los equipos y la información.
- El Centro de Procesamiento de Datos no cuenta con salida de emergencia. Al no contar con salida de emergencia la vida de los empleados del CPD y los equipos e información del mismo se ven gravemente amenazados al producirse un incendio u otro incidente que bloquee la entrada del mismo.
- No se cuenta con una política documentada para la gestión de claves de acceso, esto se lo realiza basado en la experiencia del administrador de sistemas. Al no

existir una política documentada para la gestión de claves se puede facilitar: adivinar o descubrir la clave mediante alguna técnica de ingeniería social, lo que permitiría a una persona no autorizada acceso a recursos de información de uso de la empresa.

- No existe registro de los intentos de aceptación y rechazo de claves, no se realiza seguimiento a los registros de accesos no autorizados y autorizados. No se puede determinar el número de accesos de los usuarios y si estos fueron autorizado o negados, evitando detectar intentos de posibles accesos maliciosos.
- No se llevan registros de los procedimientos que se sigue cuando el usuario está de vacaciones, ha olvidado su contraseña o qué hacer con claves sin usar. La persona encargada de estos procedimientos puede omitir involuntariamente alguna acción a realizar en estos casos, dejando en condiciones de vulnerabilidad las claves involucradas.
- No se guarda los passwords usados por el usuario. El usuario podría usar uno anterior que tal vez ya haya sido revelado o descubierto por técnicas de ingeniería social, ya que no existe restricción en el uso de passwords anteriores.
- La empresa no ha establecido un procedimiento de capacitación continua para el personal. Desconocimiento por parte del personal de las nuevas vulnerabilidades, virus y métodos de ingeniería social que podrían afectar la seguridad del CPD.
- Diagrama de topología de la red desactualizado, debido a la falta de tiempo y de personal que se dedique a la documentación. No se cuenta con un diagrama actualizado de la red que muestre de manera visual la ubicación de los equipos de la red a través de las dependencias de la empresa.
- No se cuenta con un respaldo en caso de la caída del servidor y de pérdida de información. Con la caída del servidor se produce la paralización de los servicios de la empresa, produciéndose daños económicos y pérdida de información importante.
- Si bien se hacen chequeos periódicos de la red, la ejecución de estos y sus resultados no se documentan, se limita a un informe de resultados enviados a través del correo.

  No se tiene un histórico de las pruebas y sus resultados, que permitan conocer los aspectos de la red que producen problemas para conocer si las medidas tomadas fueron o no efectivas.
- En las bases de datos no se controla los siguientes puntos:
    - Tiempo y duración de los usuarios en el sistema.
    - Número de intentos fallidos de conexión a la base de datos.
    - Ocurrencias de bloqueo (deadlock) con la base de datos.
    - Estadísticas de entrada salida para cada usuario.

- No es posible determinar el tiempo y frecuencia con la que los usuarios utilizan los sistemas, esto para efectos de control y estadística. No se documenta los ingresos con intenciones maliciosas por parte de usuarios no autorizados. No se puede determinar si se trata o no de olvidos de clave por parte de los empleados.
- No se han establecido procedimientos que eviten ingresar y registrar software no autorizado por parte de los empleados. Cualquier funcionario puede instalar software no autorizado y proceder a registrarlo de acuerdo a su criterio, lo que puede ocasionar problemas a la empresa incluso de carácter legal al instalar y registrar software pirata.
- No se documentan los cambios de emergencia al realizar el mantenimiento de las aplicaciones. Desconocimiento de los cambios realizados a las aplicaciones durante los mantenimientos, no se puede determinar: quien lo hizo, por qué razón se hizo los cambios, que se cambió, fecha del cambio y resultados del mismo.
- No se obtiene un backup de la configuración de los sistemas antes de hacer un cambio. Al no obtenerse un backup de la configuración, si algún problema se presenta en la implementación de los cambios no se podría recuperar la configuración anterior, ocasionando graves inconvenientes a los sistemas de la empresa, incluso la pérdida de información.
- No se documenta los cambios hechos a la configuración de los equipos. Imposibilidad de conocer: quien autorizó los cambios, quien realizó un backup de la configuración, quien hizo los cambios, fecha y hora de los cambios, a que sistema, que resultados se esperan.
- No se documenta las pruebas para los sistemas ni sus resultados. No existe un documento que describa las pruebas de testeo que se realizan a los sistemas así como los resultados obtenidos de estas pruebas, por lo que se desconoce si los resultados fueron 100 por ciento satisfactorios o existe algún tipo de problema con el sistema.
- No se ha implementado una mesa de reporte de incidentes o ayuda para los usuarios. Los usuarios no tienen un lugar específico donde acudir a reportar incidentes de seguridad y solicitar ayuda para solucionarlos, por lo que se desconoce la frecuencia con la que se presentan y las medidas para mitigar sus efectos.
- No existe en la empresa un plan de continuidad del CPD. No se conoce las acciones a llevar a cabo para garantizar la continuidad del negocio en el menor tiempo posible. Esto puede ocasionar en el caso de una emergencia grave pérdidas económicas a la empresa.

- La empresa no ha establecido un procedimiento de capacitación continua para el personal. Desconocimiento por parte del personal de las nuevas vulnerabilidades, virus y métodos de ingeniería social que podrían afectar la seguridad del CPD.
- No existe un plan documentado de recuperación de backups. Al no haber un plan de recuperación de backups, donde se describa las acciones a tomar para realizarlo, se corre el peligro que la recuperación se la realice incorrectamente o no se recupere toda la información necesaria para garantizar la operación de los sistemas.
- Existe una gran deficiencia en cuanto a la documentación de las actividades principales y secundarias del Centro de Procesamiento de Datos, debido a que no se cuenta con el personal para que se dedique a esta labor. No existe registros impresos de las actividades realizadas en el Centro de Procesamiento de Datos, por lo que no se puede justificar el trabajo realizado ya que no existe constancia del mismo, sólo existen reportes que son enviados por correo interno. Esto dificulta conocer si los problemas ya se presentaron en el pasado y las acciones correctivas tomadas que permitieron solucionarlos.
- Existe un Plan de Seguridad pero en el mismo no se incluye un Plan de Recuperación de Desastres, no se definen las responsabilidades y funciones de las personas en el plan de contingencia, no hay ningún mecanismo de reportes o historial para el manejo de incidentes, no se documenta el plan de contingencias y no se hacen pruebas del plan. Las personas involucradas no saben qué hacer para realizar la recuperación después de un desastre, no se tiene antecedentes documentados de recuperaciones de incidentes, por lo que este proceso puede ser muy largo y realizado deficientemente.
- No se cuenta con equipos de respaldo que puedan en caso de una emergencia o daño de los equipos principales mantener en funcionamiento los sistemas de los que depende la empresa. En caso de una emergencia grave no sería posible mantener operativa la empresa y el tiempo en que se lo podría hacer es muy largo, ocasionando grandes pérdidas económicas a la empresa.
- No existe en la empresa un plan de Recuperación del Centro de Procesamiento de Datos. No se conoce las acciones a llevar a cabo para garantizar la continuidad del negocio en el menor tiempo posible. Esto puede ocasionar en el caso de una emergencia grave pérdidas económicas a la empresa.

6.2 Recomendaciones.

- Es conveniente de que a los visitantes no se les permita deambular por otras áreas de la empresa y que la puerta del CPD se mantenga con llaves, dando una copia de las mismas solo al personal que labora en el mismo. También se puede instalar una cámara extra al circuito cerrado de televisión que grabe el acceso al centro de cómputo o modificar la orientación de alguna cámara cercana hacia la puerta de ingreso.
- Se debería instalar sistemas de detección de humo, fuego e intrusos como complemento a las medidas constructivas contra incendios.
- En lo posible considerar la posibilidad de cambiar al centro de procesamiento a un piso alto para garantizar la protección de los equipos e información en el caso de una inundación. O en su defecto implementar un sistema de alarma temprana ante la posibilidad de inundación para trasladar los equipos a un lugar seguro; para proteger los equipos en caso de incendio se debe considerar el cambio de los materiales del piso y techo por otros de tipo ignífugo y la instalación de sistemas de extinción por aerosol.
- Cambiar la ubicación del CPD a un espacio diseñado para garantizar la seguridad física de empleados, equipos e información. De no ser posible hacerlo, considerar la construcción de una salida de emergencia debidamente rotulada y con las seguridades del caso.
- Documentar adecuadamente la política de la empresa en cuanto a la gestión de claves de acceso determinando las medidas de gestión y protección de contraseñas, normas para proteger las contraseñas, normas para elegir contraseñas.
- Mantener un registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado no autorizado, que permita la revisión mensual por parte del encargado de la seguridad, a fin de detectar posibles intentos de acceso por usuarios no autorizados o problemas de los usuarios con sus claves.
- Documentar adecuadamente los procesos a seguir en los casos en los que le funcionario se encuentre de vacaciones, ha olvidado su contraseña y las claves sin usar, para garantizar la seguridad en la gestión de las claves de acceso.
- Se debe mantener un archivo con los password utilizados por los usuarios con la finalidad de no permitir su uso cuando el usuario cambie el mismo, ya que este podría haber sido revelado.
- Establecer un programa de capacitación continua que permita al personal estar actualizado en el conocimiento de las nuevas vulnerabilidades y las acciones de mitigación.

- Elaborar un diagrama topológico de la red, ya que el gráfico es mucho más fácil de entender y da una visión amplia de la red en comparación con la descripción escrita de la topología de red.
- Implementar lo más rápido posible un sistema de respaldo de emergencia que permita mitigar la pérdida de información y daños económicos para la empresa.
- Implementar un proceso de documentación de los chequeos de la red, donde como mínimo incluya: nombre del responsable, fecha, novedades y acciones a implementar para corregir los problemas detectados.
- Establecer una política que permita registrar y documentar los accesos al sistema, el número de intentos fallidos de conexión a la Base de Datos, ocurrencias de bloqueo, con la finalidad de implementar un control estadístico del uso de la Base de Datos y los sistemas.
- Establecer la política de no permitir instalar software sin autorización y describir los pasos a seguir para registrar el software autorizado.
- Al realizar el mantenimiento de aplicaciones, si se tiene que realizar algún cambio este debe ser debidamente documentado e informado.
- Obtener backups de la configuración de los sistemas antes de realizar cambios en los mismos, estos deben ser debidamente etiquetados y guardados.
- Documentar adecuadamente los cambios realizados a los sistemas, con la finalidad de contar con un archivo histórico de los mismos y poder recuperar la configuración anterior si es necesario.
- Documentar las pruebas de testeo de los sistemas en la que incluya: Tipo de prueba, datos de prueba usados, fecha y hora de las pruebas, quien las realizó, los resultados de las mismas fueron favorables o desfavorables, observaciones y recomendaciones.
- Definir claramente a donde tienen que acudir los usuarios a reportar incidentes de seguridad y solicitar asesoramiento de las acciones a seguir con la finalidad de reducir o eliminar estos sucesos.
- Realizar lo más pronto posible un Plan de Continuidad para el Centro de Procesamiento de Datos en el que se describa como mínimo: Objetivo, actividades, responsables, etc.
- Establecer un programa de capacitación continua que permita al personal estar actualizado en el conocimiento de las nuevas vulnerabilidades y las acciones de mitigación.
- Elaborar un plan de recuperación, describiendo los pasos y acciones que garanticen la correcta recuperación de la información.

- Todas las actividades del Centro de Procesamiento deben ser documentadas por escrito y mantenidas en un archivo adecuado tanto magnético como físico de tal forma de poder consultarlas en caso de requerirlo.
- Completar el Plan de Seguridad de manera que contenga por lo menos:
    - Objetivos del plan.
    - Modo de ejecución.
    - Tiempo de duración.
    - Costes estimados.
    - Recursos necesarios.
    - Evento a partir del cual se pondrá en marcha el plan.
    - Personas encargadas y sus responsabilidades
- Mantener equipos con la configuración similar a los equipos principales, de manera que puedan ser utilizados como servidores en caso de una emergencia. Garantizando la continuidad del negocio.
- Realizar lo más pronto posible un Plan de Continuidad para el Centro de Procesamiento de Datos en el que se describa como mínimo: Objetivo, actividades, responsables, etc.

Bibliografía

Aguirre, X. (2011). *Redes Configuración y Topologia*. Recuperado de http://www.slideshare.net/cenedis/redes-configuración-y-topologia

Auditoria. (2011). *Seguridad Lógicay Confidencial*. Recuperado de http://muziek-film-kunst.blogspot.com/2011/01/seguridadlogica-y-confidencial.html

Canales, C., & Marroquín, K. (2012). *Administración y Recuperación de desastres*. Recuperado de http://administraciónycentrosdecomputo.blogspot.com/2012/11/recuperacion-de-desastres.html

Castro, G., Díaz, G., Alzórriz, I., & Sancrsitóbal, E. (2014). *Procesos y Herramientas para la Seguridad de Redes.* Madrid: Universidad Nacional de Educación a Distancia.

Contreras, N., & La Rosa, C. (2011). *Enfoque de la Seguridad de la Información Curso Seguridad Informática*. Recuperado de http://es.escribd.com/doc/59484913/Historia-de-la-Seguridad-a

Coronel, C., Steven, M., & Rob, P. (2011). *Base de Datos Diseño, implementación y administración.* México: Cengage Learning S.A.

Estebañez, M., Ibañez, M., & Manzano, A. (2012). *Topología de Redes - Aspectos a tener en cuenta en una topología*. Recuperado de http://ammfico.blogspot.com/2012/01/aspectos-tener-en-cuenta-en-una.html

Gil, P., Pomares, J., & Candelas, J. (2010). *Redes y Transmisión de Datos.* Alicante: Universidad de Alicante.

Gobernance Institute. (2007). CobiT 4.1 Marco de Trabajo, Objetivos de Control, Directrices Generales, Moelos de Madurez.

Gómez Vieites, A. (2011). *Seguridad en Equipos Informáticos.* Madrid: Starbook.

Gómez, A. (2011). *Enciclopedia de la Seguridad Informática 2da Edición.* España: GaliNova.

Hernández, R. (2003). *Administración de la función Informática una nueva profesión.* México: Limusa S.A.

Huertas, V. (2011). *Tecnología: Los virus tambien avanzan*. Recuperado de http://valentinahuertas.blogspot.com/2011/04/caracteristicas.html

Mattos, E. (2010). *Seguridad en el comercio electronico. Tesis Digitales UNMSM*. Recuperado de http://sisbib.unmsm.edu.pe/bibvirtualdata/cap2.PDF

Mujica, M. (2010). *Seguridad Informática*. Recuperado de http://www.slideshaer.net/mmujica/seguridad-informatica-live-cd

Piattini, M. (2008). *Auditoria de Tecnologías y Sistemas de Información.* Madrid: Ra-Ma.

Portillo, K. (2014). *Gerencia de Sistemas - Grupo 3*.

Recuperado de https://prezi.com/d-ullo_dhs4/universidad-dr-andres-bello/

Revista Tecnológica Aplicaciones Ingeniería ITSC. (2011).
Recuperado de http://www.itscoalcoman.edu.mx/

Stallings, W. (2004). *Fundamentos de Seguridad en Redes, Aplicaciones y Estándares.* Madrid: Parson Educación.

Tanenbaum, A. (2003). *Redes de Computadoras.* México: Pearson Educación.

Universidad Autonóma de Yucatan. (2011). Ciclo de vida de un virus. Yucatán, México.

Universidad Autónoma de México. (sf). Administración de Redes.
Recuperado de http://redyseguridad.fi-.unam.mx/proyectos/asmonredes/PHP/capitulo1.html

ANEXOS.

Anexo 1. Cronograma Auditoría Seguridad.

	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
Seguridad Física	Elaboración cuestionario	3	10-12-2012
	Aplicación encuesta	2	15-12-2012
	Análisis cuestionario	5	20-12-2012
	Determinar debilidades	2	25-12-2012
	Determinar efectos	2	27-12-2012
	Elaborar Recomendaciones	1	29-12-2012
	Informe Seguridad Física	2	02-01-2013

	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
Seguridad Lógica	Elaboración cuestionario	3	07-01-2013
	Aplicación encuesta	2	12-01-2013
	Análisis cuestionario	2	14-01-2013
	Determinar debilidades	2	21-01-2013
	Determinar efectos	2	23-01-2013
	Elaborar Recomendaciones	1	25-01-2013
	Informe Seguridad Lógica	2	27-01-2013

	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
Seguridad de la Red	Elaboración cuestionario	3	28-01-2013
	Aplicación encuesta	2	02-02-2013
	Análisis cuestionario	5	04-02-2013
	Determinar debilidades	2	09-02-2013
	Determinar efectos	2	11-02-2012
	Elaborar Recomendaciones	1	12-02-2013
	Informe Seguridad de la Red	2	14-02-2013

	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
Seguridad Aplicaciones	Elaboración cuestionario	3	15-02-2013
	Aplicación encuesta	2	18-02-2013
	Análisis cuestionario	5	20-02-2013
	Determinar debilidades	2	22-02-2013
	Determinar efectos	2	24-02-2013
	Elaborar Recomendaciones	1	25-02-2013
	Informe Seguridad Física	2	27-02-2013

	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
Administración CPD	Elaboración cuestionario	3	02-03-2013
	Aplicación encuesta	2	04-03-2013
	Análisis cuestionario	5	06-03-2013
	Determinar debilidades	2	11-03-2013
	Determinar efectos	2	13-03-2013
	Elaborar Recomendaciones	1	15-03-2013
	Informe Seguridad Física	2	16-03-2013

	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
Plan de Seguridad	Elaboración cuestionario	3	18-03-2013
	Aplicación encuesta	2	21-03-2013
	Análisis cuestionario	5	23-03-2013
	Determinar debilidades	2	28-03-2013
	Determinar efectos	2	30-03-2013
	Elaborar Recomendaciones	1	01-04-2013
	Informe Seguridad Física	2	02-04-2013

Informe Final	ACTIVIDAD	DURACIÓN (DÍAS)	FECHA
	Elaboración Informe Auditoria	8	03-04-2013

Anexo 2. Entrevista Seguridad Física.

1. Controles de Acceso al Centro de Cómputo

- ¿Realizaron un análisis costo beneficio a la hora de implementar los controles?
  SI ¿Cómo se asesoraron? .....
  NO ¿Por qué? .....
- ¿Restringen el acceso al centro de cómputo a las personas que no pertenecen al mismo? ¿Qué métodos de control aplican? ¿Dónde?
  Tarjetas de entrada.....
  Guardias de seguridad.....
  Llaves Cifradas.....
  Circuito cerrado de televisión.....
- ¿Qué tipos de autenticación se utiliza en la empresa?
  Con algo que el individuo sabe (password, PIN, etc.)
  Algo que el individuo procesa (un token, un smart card, etc.)
  Algo que el individuo es (controles biométricos)
  Algo que sabe hacer (como los patrones de escritura)
- ¿Por qué no utilizan las otras?
  Por el costo ----
  No vale la pena ----
- ¿Dejan entrar solo a personal que lo necesite? SI ---- NO----
- ¿Les hacen algún control? ¿Cuál? .....

2. Control de Acceso a los Equipos

- ¿Cómo se controlan los siguientes accesos?
  La BIOS tiene habilitada una contraseña SI ---- NO ----
  Las Pc's tienen habilitadas:
  La unidad de CD o DVD SI ---- NO ----
  La lectora de tarjetas de memoria SI ---- NO ----
- ¿Cómo se controlan estos dispositivos? .....
- ¿De qué manera se evitan los virus en los CD's y Memorias? ….....
- ¿Estos dispositivos son booteables (se permite desde el setup el booteo de estos dispositivos? SI---- NO ----
- ¿ Ha habido robos de información a través de estos dispositivos ? SI ---- NO ----
- ¿Las unidades de Memoria, CDW y DVD RW están habilitadas en todos los equipos? SI ---- NO ----
- ¿Quién tiene acceso a ellos? …….....

- ¿En qué máquinas están?

  .....

- ¿Los dispositivos externos extraíbles están guardados con llaves? SI ---- NO ----
- ¿Existe control sobre terceros que realizan mantenimiento? SI ---- NO ----
- ¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados? SI ---- NO ----
- ¿Puede alguien instalar una impresora u otro dispositivo (un zip o disco removible) en alguna máquina? SI ---- NO ----
- ¿Cómo se hace el control de dispositivos que se instalan en las Pc's ?

  ¿Se hace una revisión periódica de los mismos? .....

  ¿Quién las hace? .....

  ¿Cada qué tiempo? .....

- ¿Se apagan los servidores en algún momento? SI ---- NO ----
- ¿Es necesario que queden prendidos las 24 horas? .....

3. Unidades de soporte

- ¿Cuenta el CPD con los siguientes elementos?

  Aire Acondicionado (18o C a 20oC) SI ---- NO ----

  Calefacción SI ---- NO ----

  Control de humedad (65 por ciento) SI ---- NO ----

  Luz de emergencia en el centro de cómputo SI ---- NO ----

  Detectores de humo, agua y calor SI ---- NO ----

  Alarmas:

  contra fuego SI ---- NO ----

  humo SI ---- NO ----

  calor SI ---- NO ----

  intrusos SI ---- NO ----

  agua SI ---- NO ----

- ¿Qué otras hay?

  Servidor de repuesto o redundante SI ---- NO ----

  UPS SI ---- NO ----

  ¿Cuántos? .....

  ¿En qué máquinas? .....

  ¿Funcionando cuántas horas? .....

  Estabilizador de tensión SI ---- NO ----

  ¿Cuántos? .....

  ¿En qué máquinas? .....

Extintores de incendio:

¿Son los adecuados? SI ---- NO ----

¿Son manuales o automáticos (rociadores)? .....

¿Se corta la energía eléctrica cuando se activan estos rociadores? SI---- NO

¿Están en el lugar correcto? SI ---- NO ----

¿En qué lugares?.....

¿Cómo eligieron el lugar ? .....

- ¿Se revisan las posibles fallas eléctricas o posibles causas de incendio? SI ---- NO -
- ¿Se cubren los equipos cuando se activan los rociadores? SI ---- NO ----
- ¿Hay una sola red eléctrica? SI ---- NO ----
- ¿Hay equipos que eviten la sobrecarga de la red eléctrica? SI ---- NO ----
- ¿Hay hardware especial de aislamiento y protección de dispositivos magnéticos? SI ---- NO ----

4. Edificio

- ¿El edificio fue diseñado tomando en cuenta la seguridad de los datos y equipo? SI ---- NO ----

Centro de cómputo:

- ¿Está ubicado en pisos elevados (para prevenir inundaciones)? SI ---- NO ---
- ¿Existe piso o techo falso para pasar el cableado? SI ---- NO ----
- ¿El piso o techo falso están fabricados con materiales incombustibles? SI ---- NO ----
- ¿El área que cubre el piso o el techo falso es de fácil acceso? SI ---- NO ----
- ¿El piso y techo del centro de cómputo es impermeable? SI ---- NO ----
- ¿Es lo suficientemente grande previendo el crecimiento de la red o re instalaciones ? SI ---- NO ----
- ¿La localización del centro de cómputo tiene paredes incombustibles? SI ---- NO ----
- ¿Está cerca del backbone? SI ---- NO ----
- ¿El personal está capacitado para actuar en caso de incendio? SI ---- NO ----
- ¿Está permitido comer, fumar o beber dentro del centro de cómputo? SI ---- NO ----
- ¿Existen procedimientos estándar para la recepción y almacenaje de papel? SI ---- NO ----
- ¿El Departamento de Bomberos de su localidad está al tanto de las particularidades y Vulnerabilidades del Centro de Cómputo? SI ---- NO ----

Cableado

- ¿Usan cableado estructurado? SI ---- NO ----
- ¿Utilizan alguna norma para el cableado? .....

- ¿Se consideró la ubicación de los canales, para que sean afectados por inundaciones, cortes eléctricos, desagües o campos magnéticos? SI ---- NO ----
- ¿Utilizan cables especiales para que no haya interferencia? SI ---- NO ----
- ¿Qué medidas utilizan para controlar las interferencias?.....
- ¿Cómo previenen los cortes o daños en los cables?.....
- ¿Cómo calcularon el ancho de banda de la red?.....
- ¿Es suficiente? SI ---- NO ----
- ¿Las bocas de red son suficientes? SI ---- NO ----
- ¿Cuántas utilizan? .....
- ¿Cómo protegen las que no utilizan?
  ¿Están habilitadas? SI ---- NO ----
  ¿Cómo las deshabilitan? .....
- ¿Se conoce por donde van las cañerías de forma que no interfieran con la red? SI --- NO ----
- ¿El Centro de Cómputo esta cerca o aledaño a áreas donde se utiliza o almacene materiales inflamables, tóxicos o corrosivos? SI ---- NO ----
- ¿El mobiliario del centro de datos está fabricado con materiales inflamables? SI ---- NO ----
- ¿Existe alguna forma de cortar la energía inmediatamente en caso de emergencia? SI ---- NO ----

Anexo 3. Entrevista Seguridad Lógica.

1. Identificación de usuarios.

Altas:

- ¿Qué datos se guardan en el perfil de usuario?:
  ID del usuario -----, tiene relación con código de recursos humanos SI---- NO----
  Password ----
  Apellidos y Nombres ----
  Departamento o Unidad a la que pertenece ----
  Fecha de expiración del password ----
  Fecha de anulación de la cuenta ----
  Contador de intentos fallidos ----

Bajas:

- ¿Recursos humanos informa las desvinculaciones y cambios de funciones del personal? SI---- NO ----
- ¿Existen procedimientos para la eliminación de claves? SI ---- NO ----
  ¿Se llevan registros de las claves eliminadas? SI ---- NO ----
  ¿Por cuánto tiempo? .....
  ¿Qué datos se guardan? .....
  ¿Con qué finalidad? .....
- ¿Estos procedimientos se realizan inmediatamente después que el empleado se ha retirado de la empresa? SI ---- NO ----

Gestión y Mantenimiento:

- ¿Cuentan con una política documentada para la gestión de claves de acceso? SI ---- NO ----
- ¿Quién es la persona encargada de administrar las claves? SI ---- NO ----
- ¿Cómo están conformadas las claves de acceso? .....
- ¿Con qué periodicidad se actualizan las claves? .....
- ¿Son utilizadas técnicas de cifrado para proteger las claves? SI ---- NO ----
- ¿Se verifica que el usuario tenga autorización para el uso del sistema antes de asignarle una clave? SI ---- NO ---- ¿Quién autoriza? .....
- ¿En caso de que el usuario cambie de función, se lleva un registro actualizado de los cambios de privilegios? SI ---- NO ----
- ¿Existe un registro de los intentos de aceptación y rechazo de claves de usuario en el sistema? SI ---- NO ----
- ¿Existe un registro que indique la hora, fecha y aplicación que utilizo el usuario? SI ---NO ----

- ¿Se realizan seguimientos a los registros de accesos no autorizados, autorizados y fallidos? SI ---- NO ----
- ¿Existen registros de errores al ingresar datos, por cada aplicación? SI ---- NO ----
- ¿Está el tiempo de conexión limitado al horario de trabajo? SI ---- NO ----
- ¿Qué procedimientos se sigue cuando el usuario se encuentra dentro de alguna de estas condiciones?:
  Vacaciones.....
  Olvido o revelación de claves.....
  Claves sin usar.....
- ¿Se llevan registros de estos procedimientos? SI ---- NO ----

2. Autenticación

- ¿Qué se muestra cuando se tipea el password?
  Asteriscos ----
  Espacios ----
  No se mueve el cursor ----
- ¿Cómo se guardan los datos de autenticación?
  Encriptados ----
  Bajo password ----
- ¿De qué forma se los asegura? …….....
- ¿Se clasifica estos datos como confidenciales? SI ---- NO ----
- ¿Quién tiene acceso a estos datos? .....
- ¿La autenticación es para: toda la red ---- o por aplicación ----?
- ¿Se bloquea el acceso luego de un número de intentos fallidos? SI ---- NO ----
  ¿Después de cuantos intentos de acceso? .....
- ¿El equipo espera un tiempo para mostrar nuevamente la ventana de ingreso de contraseña? SI ---- NO ----
- ¿Se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos? SI ---- NO ----
- ¿Y para mensajes externos? SI ---- NO ----
- ¿Serian necesarias para algún documento? SI ---- NO ----

3. Password

- ¿Qué método emplean para generar las claves?
  Software ----
  Usuario ----
- ¿Qué características debe tener el password?
  Caracteres permitidos.....

Tamaño mínimo y máximo…….....

- ¿El password se inicia como expirado para obligar el cambio? SI ---- NO ----
- ¿Se permite que tenga el nombre de la empresa, o el nombre del usuario? SI ---- NO ----
- ¿Dos cuentas pueden tener el mismo password? SI ---- NO ----
- ¿De existir dos o más cuentas de administrador, todas o algunas de ellas tienen el mismo password? SI ---- NO ----
- ¿El password puede ser el mismo que el ID del usuario? SI ---- NO ----
- ¿Con que frecuencia es necesario cambiar el password antes de que se vuelva obsoleto?.....
- ¿Se puede cambiar el password en cualquier momento? SI ---- NO -----
- ¿Cuál es el procedimiento para manejo de password pérdidas o reveladas? :
  ¿Se guarda los password usados por el usuario? SI ---- NO ----
  ¿Cuántos password de cada usuario se guardan? .....
  ¿Se capacita a los usuarios sobre la administración del password? SI ---- NO ----
- Se les enseña a:
  No usar password fáciles de descifrar ----
  No divulgarlas ----
  No escribirlas o guardarlas en lugares fáciles de encontrar ----
  No usar la misma clave para varios servicios ----
  Comprender que el password es el principal método de seguridad ----

4. Roles

- ¿Las claves se asignan por grupos de usuarios ---- o por cada usuario ----?
- ¿Los permisos de (lectura, escritura, ejecución, eliminación, todos los anteriores) son asignados de acuerdo a las funciones del usuario? SI ---- NO ----
- El ID hace referencia:
  A una persona ----
  Anónimos ----
  Al grupo ----

5. Transacciones

- ¿ Se permite hacer ciertas transacciones a unos usuarios que otros no pueden hacer? Dependiendo de:
  Tipo de usuario—
  Del Grupo—
- ¿Se restringe el acceso a ciertos programas a ciertos usuarios? SI ---- NO ----
  ¿Cómo?.....

6. Limitaciones a los servicios

- ¿Existe en la empresa productos de software cuya licencia limite su uso a un número determinado de usuarios? SI ---- NO ----
- ¿El administrador ha establecido límites al uso simultaneo de ciertas aplicaciones? SI ---- NO ----

7. Modalidad de acceso

- ¿Existe un procedimiento para la asignación de permisos de acceso? SI ---- NO ----
- Se los asigna por: Usuario ----, Aplicación -----.
- ¿Quién otorga estos permisos y con qué criterios? .....
- ¿Está documentado este procedimiento? SI ---- NO ----

8. Ubicación y horario

- ¿Está el tiempo de conexión limitado al horario de trabajo? SI ---- NO ----
- ¿Se restringe el acceso a determinadas horas del día o días de la semana para mayor control? SI ---- NO ----
- ¿Son necesarias estas restricciones de acceso? SI ---- NO ----

9. Control de acceso interno

- ¿Cuál mecanismo de control de acceso se utilizan?
  Password ----
  Listas de Control de acceso ----
  ¿Con qué aplicaciones se manejan?.....
  ¿Cómo se actualizan?.....
  ¿Con qué frecuencia se revisa o actualiza?.....
  ¿Se usa encriptación para almacenarla?.....
- Interfaces de usuarios restringidas:
- ¿Solo ven lo que les está permitido? SI ---- NO ----
- ¿Cómo se hacen las restricciones? ¿Con la vista de menús? SI ---- NO ----
- ¿De qué otra forma? .....
- Encriptación: ¿Se encriptan algunos datos? SI ---- NO ---- ¿Cuáles?
  Las listas de control de acceso ----
  Los mensajes ----
  Los passwords y las cuentas de usuario ----
  Los datos de configuración ----
  Los datos críticos de la empresa ----
  Los datos que están siendo transmitidos ----

10. Control de acceso externo

- Mecanismos de control de acceso externo:

Gatewas o firewalls seguros ----

Acceso de personal contratado, consultores y mantenimiento ----

Autenticación basada en host ----

- ¿Existe acceso externo a los datos, desde internet ----- o desde módem -----?
- ¿Quién tiene acceso? .....
- Para mantener la integridad y confiabilidad de los datos, se tiene en cuenta:

  ¿Alguna forma de identificación y autenticación? -----

  ¿Control de acceso para limitar lo que se ve, lee, borra, modifica, etc? -----

  ¿Firmas digitales? ----

  ¿Guardan las copias de seguridad de información pública en otro lado, no en la misma máquina? ----

  ¿Prohíben el acceso público a bases de datos vivas? ----

  ¿Verifican que los programas y la información pública no tengan virus? -----

  ¿Están separados los datos que se publican en internet de los datos internos de la empresa? ----

  ¿Usan alguna firma de acceso remoto para cambiar la configuración del sistema? ----

11. Administración de personal

- ¿Se tiene una máxima separación de funciones? ----
- ¿Se otorga el mínimo permiso de acceso requerido para cada puesto? ----
- ¿Se considera los requerimientos de experiencia y conocimiento para cada puesto? ----
- ¿La empresa tiene establecido un procedimiento de capacitación continua para el personal? ----
- ¿El personal tiene conciencia de la importancia de la información como recurso valioso para la empresa? ----

Anexo 4. Entrevista Seguridad de la Red.

1. Activos de la Red

- ¿Cómo es la topología de la Red?.....
- ¿Existe un inventario o gráfico de la topología? SI — NO — Este incluye:
  Switch ----
  Routers ----
  Hub's ----
  Modem ----
  Pc's ----
  Conexiones de radio ----
  Fibra óptica ----
  Cable UTP ----
- ¿Cuántos dispositivos de la lista hay y en qué forma están ubicados y utilizados?

.....

- ¿Qué filtros tiene cada uno de los dispositivos?.....
- ¿Existe encriptación a nivel de hardware? SI ---- NO ----
- ¿Tiene switch? SI ---- NO ----
- ¿Por qué pusieron switch en lugar de un router? ¿Por el costo? ----- ¿ Por el tamaño de la Red ? -----
- ¿Tienen sistema radial ? ¿ Por qué implementaron un sistema radial ?
  .....
  ¿Es muy inseguro? SI ---- NO ----
  ¿ No es muy caro? SI ---- NO ----
- Servidor de hosting
  ¿Qué se tuvo en cuenta para elegir el servidor de hosting?
  Precio ----
  Medidas de seguridad ----
  Respaldo en caso de emergencia, de caída del servidor y pérdida de información ----
- ¿Qué características tienen los servidores ? (de mail, de internet, de datos o aplicaciones) .....

Comunicaciones - Modem

- ¿Pasa por el firewall? SI ---- NO ----
- ¿Los datos van encriptados? SI ---- NO ----
- ¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a internet? SI ---- NO ----

Recursos Compartidos

- ¿Se comparten los discos de las PC's en la red? SI ---- NO ----- ¿Por qué? ¿Qué carpetas comparten ?.....
- ¿Se puede ver las carpetas de los mails de los compañeros de trabajo? SI ---- NO ---- ¿Tienen contraseñas estas carpetas? SI ---- NO ----
- ¿Quién pone las contraseñas: el dueño de la información o el administrador? …….....

Fiabilidad

- ¿Existen medios alternativos de transmisión de datos en caso de que ocurra alguna contingencia con la red? SI ---- NO ----
- ¿Qué se haría si se cae un nodo?……
- ¿Está prevista esta situación? SI ---- NO ----
- ¿Existe redundancia de acceso a internet? SI ---- NO ----

Configuración de puertos

- ¿Se deshabilitaron los puertos que no son necesarios? SI ---- NO ---- ¿Cuáles? .....……¿De qué protocolos o servicios? .....¿Quién lo hizo?.....
- ¿Se prueban los puertos de la red? SI — NO — ¿Y el firewall? SI — NO —
- ¿Con qué herramientas? .....
- ¿Se ha hecho una prueba de autohaqueo? SI — NO —
- ¿Con que herramientas se prueban o pueden borrar los puertos? …….....
- ¿Qué programa usaron? .....

Chequeo de red

- ¿Se hace algún chequeo periódico de la red y sus permisos? SI ---- NO ----
- ¿Qué se controla? .....
- ¿Se documenta la ejecución y los resultados de estas pruebas? SI ---- NO ----

Mail-Chat, Herramientas

- ¿Con que herramienta administran el correo y como se hace?
  ¿Es una herramienta del sistema operativo? ----
  ¿Es comprada? ----
  ¿Por qué la eligieron? …….....
  ¿Es configurable? SI ---- NO ----
  ¿Quién es el encargado de su configuración? …….....
- ¿Se chequea periódicamente que la configuración sea eficiente? SI ---- NO ----
- ¿Con qué frecuencia?..... ¿Se encuentran errores? .....
- ¿Se actualizan a las versiones nuevas de esta herramienta? SI ---- NO -----

- ¿Cómo se enteran de las nuevas versiones? .....
- ¿El servidor de mail es el mismo que el servidor de internet o el de aplicaciones? SI ---- NO---¿Con que herramienta los usuarios leen sus mails?.....
- ¿Lo hacen desde sus PC's ? SI ---- NO ----
- ¿Qué configuraciones tienen estas herramientas?
  Habilitada la vista previa ----
  Confirmación de lectura ----
  Chequeo de virus en correo entrante y saliente ----
  Controles Activex y script ----
- ¿Quién las configura? ¿El usuario ----- o el administrador -----? ¿Todas las PC's tienen la misma configuración? SI ---- NO ----

Proceso de recepción y envío de mails

- ¿Cómo es el proceso de recepción de mail? ¿El servidor baja los mails de toda la empresa a sus discos, y luego los reparte a sus destinos? SI ---- NO ----
- ¿Los mails se borran del servidor cuando son descargados a la máquina del usuario? SI ----NO ---- ¿O no se borran nunca del servidor? ------
- ¿Los mensajes están comprimidos dentro del servidor? SI ---- NO ----
- ¿Automáticamente se envían los mail a cada cuenta de usuario cuando llegan al servidor ---- o se guardan en disco del servidor y se envían en un determinado momento (por ejemplo, varias veces al día -----, o cuando el usuario lo solicita -----)?
- Al recibir cualquier tipo de mail, ¿existen mecanismos de filtrado que nos permiten buscar ciertas frases o palabras dentro del encabezado o cuerpo del mensaje? SI ---- NO ----
- ¿Podemos determinar si hay algún mail con un determinado asunto, de manera de evitar los virus o los correos no deseados? SI ---- NO ----

Espacio en disco

- ¿Cómo se administra la capacidad de disco asignada a los mails?
  ¿Se asigna un espacio de disco a la totalidad del correo? ----
  ¿Se asigna un espacio de disco a cada usuario del mail? ----
  ¿Se asigna un espacio de disco a cada cuenta de mail? ----
  ¿Se asigna un espacio de disco a cada departamento? ----
- ¿Existen distintas cantidades asignadas a los usuarios de acuerdo a su perfil o grupo --, o todos los usuarios tienen la misma cantidad de espacio en disco ----?
- ¿Qué pasa si se llega al límite de espacio en disco asignado?
  .....

- ¿Ha pasado alguna vez? SI ---- NO ---- ¿Se le avisa al usuario correspondiente que limite el uso de su cuenta de mail? SI ---- NO ---- ¿Se puede suspender solo su servicio de mail sin afectar el resto de la empresa? SI ---- NO ----
- ¿Cuándo se suspende la recepción de mails? ¿Cuándo se ha llenado el servidor ---- o antes -----, para poder hacer algo para vaciarlo?
- ¿Existe un límite para los mensajes de salida o de entrada? SI ---- NO ----

Mail Interno y Externo

- ¿Existen direcciones de mail para todos los empleados? SI ---- NO ----
- ¿De qué depende este servicio? …….....
- ¿Ese mail es interno? SI ---- NO ----
- ¿Existe una casilla para mail externo para cada empleado? SI ---- NO -----
- ¿Cómo funciona el mail interno, va al hosting ---- y después al servidor de correo ------ o va directamente al servidor de correo ----?
- ¿Existe algún tipo de control para asegurarse que los usuarios no usan el mail de la empresa para fines personales sino para su trabajo? SI ---- NO ----
- ¿Se controla que no se suscriban a listas de correo o cadenas de mails con esta dirección de mail? SI ---- NO ----
- ¿Controlan los SPAMS en estas direcciones? SI ---- NO ----
- ¿Cómo lo hacen? .....
- Al enviar mails hacia todos los empleados, ¿La lista se oculta con el CCO ----- o copia oculta, o se los lista en el campo de TO ------?
- ¿Permiten el conocimiento público de las direcciones externas de mails de los empleados? SI ---- NO ----
- ¿Están publicadas en Internet ---- o solo las administran sus propietarios ----?
- ¿Existen direcciones de mails destinadas a la comunicación con el cliente, como el libro de quejas, consultas, etc? SI ---- NO ----
- ¿En donde se encuentran? .....
- ¿Quién las administra? .....¿El departamento correspondiente ---- o el administrador de web ----?

Correo basura

- ¿Cómo se identifica al correo basura? .....
- ¿Cómo se administra el correo basura? .....
- ¿Con qué herramienta lo hacen?…….. ¿Cómo se configura? .....
- ¿Cómo se define qué es correo basura y qué no? .....
- ¿Qué pasa si a una cuenta llega gran cantidad de correo basura?

.....

- ¿El correo basura se elimina directamente ---- o es posible generar logs para su posterior análisis ----?
- ¿Qué conclusión se ha sacado de esos análisis? .....
- ¿El correo basura se baja hasta el servidor de mails y desde ahí se elimina — , o directamente se elimina antes de ser bajado— ?

Chat

- ¿Se permiten los servicios de chat? SI ---- NO ----
- ¿Cuáles se usan? MSN ----, Yahoo! ---- ¿Chat? ---- ¿Otros? ----
- ¿Se permite bajar archivos a través de estos programas? SI ---- NO ----
- ¿Se usan programas de file sharing (Morfeus, Kazaa, Napster, Audio Galaxy, iMesh, eDonkye2000, etc.)? SI ---- NO ----

Copia de seguridad

- ¿Se genera una copia de seguridad de los mensajes enviados y recibidos? SI --- NO--- ¿De todos? SI ---- NO ---- ¿Se guardan en el disco? SI ---- NO ---- ¿Se comprimen? SI ---- NO ----
- ¿Se hacen backup de las carpetas del SendMail (como las dbx del Outlook Express)? SI ---- NO ----
- ¿Se imprimen para su control o para que conste en algún archivo en papel? SI ---- NO ---- ¿Poseen un sistema propio de mail record definido o alguna herramienta automática de gestión de mails record? SI ---- NO ----

Privacidad – Firma digital – Encriptación de mails

- ¿Prohíben el envío de archivos de la empresa u otros documentos confidenciales vía mail?
- SI ---- NO ----
- ¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales? SI — NO —
- ¿Se exige que vaya firmado, o encriptado? SI ---- NO ----
- ¿Se exige que la dirección de destino sea conocida o confiable? SI ---- NO ----
- ¿Se utiliza la firma digital en algún tipo de mensajes? SI ---- NO ----
- ¿Qué tipo de firma se usa? .....
- ¿Se usa para mensajes externos e internos? SI ---- NO ----
- ¿La clave privada de la firma digital es realmente privada, o la utilizan las secretarias (por ejemplo) para mandar mensajes en nombre de sus jefes? SI ---- NO ----
- ¿Cómo se controla esto? ¿Utilizan la priorización de mail para la encriptación de los mismos? SI ---- NO ----

- ¿Qué sería importante proteger, en el caso de mensajes internos y externos?:
  Integridad ----
  Confidencialidad ----
  No repudio ----
  Autenticación del remitente ----
- ¿Se pide generalmente una confirmación de lectura en los mails salientes? SI — NO —
- ¿En todos, solo en los que tienen datos confidenciales, o cuando el usuario los configura? .....
- ¿Se encriptan los datos confidenciales que se guardan en disco (ejemplo: EFS Encrypted File System - de Microsoft)? —
  ¿Archivo con contraseñas? —
  ¿Archivos de configuración? —
  ¿Archivos top secret? —
  ¿Qué otros datos se encriptan? —

VIRUS – ANTIVIRUS, Herramientas

- ¿Cuáles de estas medidas o herramientas poseen para evitar los virus?:
  Paquetes de software antivirus ----
  Firewalls ----

  Sistemas de detección de intrusos ----
  Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos. ----
  Creación de un disco de rescate o de emergencia ----
  Procedimientos para cuando ocurra una infección con virus. ----
  Hardware de seguridad de red dedicado ----
  Backup de datos ----
- ¿Está habilitada alguna herramienta antivirus mientras se envían y reciben mails?
  SI ---- NO ---- ¿ Cuál ?.....¿ Por qué se usa esa ?
  .....
- ¿Están seguros que detecta los virus y los elimina correctamente? SI ---- NO ----
- ¿Han probado con otra herramienta? SI ---- NO ----
- ¿Hay un antivirus instalado en cada PC (incluyendo los servidores) o hay un solo antivirus en toda la red? .....
- ¿Qué significa que el antivirus sea corporativo? .....
- ¿Uno para los servidores y otra versión para los clientes? .....

- ¿En qué se diferencian?.....

Mensajes infectados – Procedimientos

- ¿Se han detectado mensajes infectados? SI ---- NO ----
- ¿Qué problemas trajo? .....
- ¿Era de Windows o de Linux? ….....¿Cómo lo solucionaron? …….....
- Si se encuentra un mail con virus, ¿Qué se hace para que no lleguen más de esa misma persona?.....
- ¿Se identifica la fuente del mail, para bloquearla desde el router o desde el servidor de correo? -----
- ¿Se avisa al ISP para que no deje entrar más mails de esa dirección? -----
- ¿Se observan los headers de los mails para identificar su origen verdadero? ----
- Si las disqueteras están activadas en las PC's de los usuarios, ¿Cómo se aseguran que los usuarios analicen los disquetes antes de abrir archivos? …….....
- ¿Se generan disco de rescate con el antivirus? SI ---- NO ----
- ¿Para todas las máquinas o solo para los servidores? ----
- ¿Quién es el encargado de esto? -----
- ¿Alguna vez han sido necesarios? SI ---- NO ----
- ¿Cómo es la protección contra el mail-bombing? ¿Qué medidas se toman? ¿Suspenden la recepción de mail cuando el servidor está ocupado en un determinado porcentaje de su capacidad?.....
- ¿Qué procedimiento siguen en el caso de una infección con un virus?..... .....
- ¿Cada cuanto se hace un escaneo total de virus en los servidores?..... ¿Quién se encarga?..... ¿Se hace automáticamente cada vez que hay una actualización o periódicamente?.....
- ¿El escaneo de las máquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas?..... ¿No sería más seguro que el encargado lo haga a intervalos regulares de tiempo? SI ---- NO ----
- ¿Qué prioridad tiene el SendMail?.....
- ¿El firewall tiene algo que ver con el análisis de los virus, o solo se encarga de los servicios de la red?

- ¿El antivirus y el firewall están relacionados de alguna forma, son compatibles entre sí? Ej. Firewall y antivirus de Norton se complementan para generar un nivel de seguridad superior?.....
- ¿Cómo se realiza el download de los mails desde el servidor hasta las PC's? ¿Cada PC se identifica según el usuario que se logea? ¿O es según el número de terminal de la PC en la red? ¿Se puede configurar una cuenta (Ej.: la de algún Gerente) en otra máquina (que no sea la del Gerente) y bajar los mails desde ahí?

Actualización de antivirus

- ¿Cómo se actualizan las definiciones de virus?.....
- ¿Quién las baja de Internet? .....
- ¿Quién ejecuta las actualizaciones en la PC's? …….....
- ¿Cómo se enteran de las nuevas actualizaciones de virus?.....
- ¿Cuánto tiempo lleva diseminar y actualizar el antivirus en toda la organización? .....
- ¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus? SI ---- NO ----

Documentación – Normas

- ¿Qué documentación existe de la red?
- ¿Diagramas topológicos? SI ---- NO ----
- ¿Procedimientos? SI ---- NO ----
- ¿Manuales? SI ---- NO ----
- ¿Certificados (Ej.: de calidad, etc.)? SI ---- NO ----
- ¿Licencias de software? SI ---- NO ----
- ¿Planes de contingencia, de seguridad, etc.? SI ---- NO ----
- ¿Contratos (Ej.: responsabilidades y mecanismos de transmisión al establecer una comunicación con las fábricas)? SI ---- NO ----
- ¿Cambios realizados en la configuración de la red? SI ---- NO ----
- ¿Qué más? .....
- ¿Poseen cada uno de estos elementos de documentación de la empresa?:
  Manual de uso del software y de hardware usado (del software desarrollado y del comprado) SI ---- NO ----
  Diagramas de red y documentación de la configuración de routers, switches y dispositivos de red. SI ---- NO ----
  Procedimientos de emergencia (plan de contingencia) SI ---- NO ----
  Plan de seguridad SI ---- NO ----

Manual de procesos estándares del Sistema Operativo (en especial de Linux) SI ---- NO ----

Métodos para compartir datos entre sistemas (por ejemplo con las fábricas, entre las sucursales o entre las PC's de la red) SI ---- NO ----

- ¿Se han instalado correctamente todos los parches de seguridad disponibles del sistema operativo y de los programas usados? SI ---- NO ----
- ¿Cómo se conoce de los parches? ¿Están suscriptos a un mailing list? SI ---- NO ----
- ¿Hay alguna documentación donde se anote la configuración de las PC's en la red? ¿Sus números IP, sus placas de red, etc.? SI ---- NO ----

Ataques de Red

- ¿Han tenido algún ataque en la red? SI ---- NO ----
- ¿Qué se ha hecho para arreglarlo?.....
- De los siguientes métodos contra los ataques más comunes, ¿Qué está implementado?

Denial of service:

¿Hay herramientas Anti DoS? -----

¿Limitan el tráfico de red? -----

¿Generan una "baseline" o líneas de base con la actividad normal del sistema? ----

¿Se hizo alguna simulación ocupando una gran cantidad de recursos de algún tipo? ----

¿Instalan los parches de seguridad del sistema operativo? ----

¿Implementan un sistema de cuotas (Disk Quotas)? -----

¿Utilizan alguna herramienta para detectar cambios en la información de configuración u otros archivos (como Tripwire)? —

Sniffing:

¿Las líneas de comunicación se segmentan tanto como sea práctico? ----

¿Los datos de logeo y otros datos sensibles son transmitidos encriptados? ----

¿Las cuentas privilegiadas (como root) se logean usando passwords one time o shadow passwords y autenticación fuerte? ----

Spoofing:

¿Tienen alguna herramienta anti-spoofing? ----

¿Los routers son configurados para que rechacen los ataques de spoofing? ----

¿Solo los hosts apropiados son definidos como confiables en el Linux (como el etc/hosts.equiv)? -----

¿Y este archivo tiene los permisos restringidos? ----

Por más que el acceso externo esté prohibido, ¿se configura el control de acceso para denegar cualquier tráfico de la red externa que tiene una dirección fuente que debería estar en el interior de la red interna? ----

Ataque a las passwords:

¿Dónde se guardan las password del sistema operativo? ¿En el archivo /etc/passwd y /etc/group ? ----

¿Se chequean regularmente las passwords para comprobar su consistencia los archivos que nombré arriba? ----

Firewall

- ¿Qué firewall usan? …….....
- ¿En qué máquina (servidor) se encuentra el Firewall? ¿En una máquina dedicada? ¿En el servidor de Internet? …….....
- ¿Qué tipo de firewall hay?
  ¿Gateway de filtrado de paquetes (Packet Filtering Gateways)? ----
  ¿Gateway de aplicación? ----
  ¿Gateways híbridos o complejos? ----
  ¿Otro?.....
- Política de configuración. ¿En base a qué criterios definieron las configuraciones del firewall?
  ¿Tienen una política definida en cuanto a la configuración del firewall? ----
  ¿Usan una política de acceso a servicios? ----
  ¿Usan una política de dial-in y dial-out? ----
- ¿Usan una política de diseño y configuración del firewall? ¿Alguna de estas dos?
  Postura de negación preestablecida. Se especifica sólo lo que está permitido y se prohíbe todo lo demás: ¿Se examinan los servicios que los usuarios necesitan? ¿Se considera como afectarían la seguridad tales servicios y como se los puede proporcionar a los usuarios de manera segura? ¿Se permiten sólo los servicios que se comprenden o se tiene experiencia, que se pueden proporcionar con seguridad y para los cuales existe una necesidad legitima? ------
  Postura de permiso preestablecido: se especifica sólo lo que está prohibido y se permite todo lo demás. -----

Características del firewall

- ¿Qué controles de acceso tiene el firewall? .....

- ¿Qué servicios tiene habilitados y cuáles deshabilitados? .....
- ¿Soporta autenticación? — ¿Con qué técnica? .....
- ¿Incluye las direcciones NAT (Network address translation) en la autenticación ? — ¿ Y passwords? ----
- ¿Qué habilidades tiene para monitorizar la red? :
  ¿Intentos no autorizados de ingreso? ----
  ¿Genera logs? ----
  ¿Provee reportes? ¿O mails? ----
  ¿Tiene alarmas? ----
  ¿Es lo suficientemente rápido para que no demore a los usuarios en sus intentos por acceder a la red (cómo es su performance)? ----
- ¿Qué tan configurables son sus opciones?
- ¿Puede adaptarse a distintas configuraciones de red o de sistemas (es escalable)? ----
- ¿Es fácil de configurar? ----
- ¿Es fácil de usar? ----
- ¿Es fácil de mantener? ----
- ¿Tiene un buen servicio postventa? ----
- Si se cae el firewall, ¿qué pasa? ¿Es una “falla segura”? ----
- ¿Se hizo alguna prueba de la configuración del firewall? ---- ¿Trató de hacerse un intento de entrada sin autorización, por ejemplo? ----

Configuración de servicios y protocolos de la red

- ¿Cuáles se usan en la red?.....
- ¿Cómo están configurados? .....
- ¿Están habilitados o prohibidos? .....
- ¿Existen excepciones? SI ---- NO ----
- ¿Poseen acceso de entrada y/o salida? SI ---- NO ----
- ¿Qué pasa con los otros puertos que quedan libres? .....
- ¿Se desactivan completamente los siguientes servicios o protocolos?
  SUID (set user ID), RLOGIN, RSH, REXEC (Comandos “r” Remote), SU (SuperUser), NetStar, GOPHER, TFTP (Trivial File Transfer Protocol), Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY. SI ---- NO ----
- ¿Cómo se configuran los siguientes servicios o protocolos?
  POP (Post Office Protocol), MIME, HTTP, SMTP, FTP, Applets, Pruebas Cgi, Scripts Query, SHELL, NIS. .....

Herramientas para administración de red y protocolos

- ¿Usan alguna de estas herramientas o protocolos para la seguridad de la red? Tcp-wrappers ----, Netlogv ----, Satan ----, AntiSniff ----, Cops ----, SafeSuite ----, Gabriel ----, Courtney ----, Tcplist ----, SSL (secure socket layer) ----, SHTTP ----, SMIME -----, NOCOL ---- (Network Operations Center On-Line).
- ¿Las herramientas que se usan tienen las siguientes funciones?
  ¿Pueden monitorear y filtrar peticiones entrantes a distintos servicios? ----
  ¿Cómo lo hacen?.....
  ¿Con qué aplicación?.....
  ¿Indican la hora, la máquina origen (el número de IP) y el puerto de esa conexión? SI ---- NO ----
  ¿Pueden seguir una traza de todos los intentos de conexión tanto admitidos como rechazados? SI ---- NO ----
  ¿Se monitorea la red buscando ciertos protocolos con actividad inusual? SI ---- NO ---

-

- Se controlan los siguientes:
  Conexiones tftp ----
  Accesos vía RSH (remote shell), ----
  Comandos en el puerto de sendmail como vrfy, expn, etc. ----
  Algunos comandos de rpc (remote procedure call) como el rpcinfo, ----
  Peticiones al servidor de NIS, ----
- ¿Se llevan estadísticas de uso de los protocolos? SI ---- NO ----
- ¿Se puede utilizar para detectar cambios en los patrones de uso de la red, y todo aquello que nos puedan hacer sospechar que algo raro está pasando en la misma? SI ---- NO ----
- ¿Se audita el tráfico IP? SI ---- NO ----
- En la captura de paquetes IP, ¿se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.? SI ---- NO ----
- ¿Tienen la posibilidad de filtrar paquetes Por hardware o por software?
  …….....
- ¿Van creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas? SI ---- NO ----
- ¿Qué otra funcionalidad no nombramos que si tiene la herramienta usada?
  .....
- ¿Qué función sería muy útil al trabajar en la red? .....
- ¿Se mantiene actualizado el software? SI ---- NO ---- ¿Se investiga para mantener actualizadas las herramientas? SI ---- NO ---- ¿Alguien está a cargo de esta

actividad? ..... ¿Se buscan herramientas nuevas?

SI ---- NO ----

Anexo 5. Entrevista Seguridad de las Aplicaciones.

1. Elección del Sistema a Usar.

- ¿Se hicieron los siguientes cuestionarios al elegir los sistemas operativos y programas usados en la empresa?
  Requerimientos funcionales: ¿qué funciones debe cumplir el sistema?----
  Entorno necesario: ¿Windows, Unix o Linux? ----
  Requerimientos de compatibilidad: ¿se ajusta a estándares o a regulaciones internacionales, o a programas existentes en la empresa? ----
  Requerimientos de perfomance: respuestas por segundo, errores, etc. ----
  Requerimientos de interoperatividad: ¿cómo se relaciona con los demás sistemas? --
  Fiabilidad: errores tolerables del sistema. ----
  Amigable: fácil de usar. ----
  Precio y precio adicional de mantenimiento. ----
  Documentación y manuales del software. ----
  Identificación y autenticación. ----
  Control de acceso. ----
  Login. ----
  Evaluación de protocolos. ----
  Incorruptibilidad. ----
  Fiabilidad. ----
  Seguridad en la transmisión. ----
  Backup de datos. ----
  Encriptación. ----
  Funciones para preservar la integridad de datos. ----
  Requerimientos sobre privacidad de datos. ----

2. Control de Datos de Aplicaciones.

- ¿Existe un control de cambios para los archivos del sistema o para las bases de datos de la empresa? SI ---- NO ----
- ¿Existen registros de datos de salida? SI ---- NO ----
- ¿Cómo es el acceso a las librerías de programa (carpeta Archivos de programas? ---
- ¿Cómo se asegura la confidencialidad de los datos en una laptop?..... ¿Qué datos hay en las laptops de la empresa, o de los usuarios?.....
- ¿Se generan logs en cada transacción de manera de poder hacer un undo? ¿Estos registran los cambios en los datos críticos del sistema? SI ---- NO ----

- ¿Se generan históricos de auditoría indicando qué los procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios - gestión de configuración)? SI ---- NO ----
- ¿Los archivos de programa y los de trabajo se almacenan en directorios separados? SI ---- NO ----

3. Control de Datos en el Desarrollo.

- ¿Se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones? SI ---- NO ----
- ¿Las variables, parámetros y/o fórmulas de cálculo se incluyen en tablas o archivos separados de los programas, para facilitar su modificación? SI ---- NO ----
- ¿Existe un proceso de control de cambios para el desarrollo? SI ---- NO ----
- ¿Cómo se documentan estos cambios? .....
- ¿Controlan el contenido de los archivos de entrada? ¿Controlan que existan los archivos antes de ejecutar el programa? SI ---- NO ----
- ¿Se hacen controles sobre la validez, de los datos ingresados manualmente? (Controles de integridad de datos). SI ---- NO ----
- ¿Se controla la consistencia de los datos de salida de las aplicaciones? SI ---- NO ---
- ¿Las aplicaciones se operan a través de menús obligatorios o es a través de los datos reales del mismo (o sea las bases de datos)? SI ---- NO ----

4. Seguridad de Bases de Datos

- ¿Los archivos de la base de datos tienen control de acceso? ¿O solo se hacen controles en las aplicaciones?.....
- ¿Se controla lo siguiente?
  Tiempo y duración de los usuarios en el sistema. ----
  Número de conexiones a bases de datos. ----
  Número de intentos fallidos de conexiones a bases de datos. ----
  Ocurrencias de deadlock con la base de datos. ----
  Estadísticas de entrada - salida para cada usuario.----
  Generación de nuevos objetos de base de datos. ----
  Modificación de datos. ----
- ¿Se hace algún chequeo regular de la seguridad de la base de datos? ¿Se documentan los chequeos? SI ---- NO ----
- ¿Se hacen y son efectivos los backups y los mecanismos de seguridad? SI ---- NO --
- ¿Hay algún usuario de la base de datos que no tenga asignado un password ? SI ---- NO ----

- ¿Hay algún usuario que no ha usado la base de datos por un período largo de tiempo?
  SI ---- NO ----
- Además del administrador de datos, ¿quién tiene acceso a los archivos del software de base de datos, a los del sistema operativo y a las tablas del sistema (FAT)?
  .....
- ¿Quién puede ejecutar un editor SQL? …….....
- ¿Quién tiene acceso de lectura - escritura a los archivos de programa?.....
- ¿Qué usuarios tienen los mismos permisos que el administrador?.....
- ¿La base de datos tiene suficientes recursos libres para trabajar?.....
- ¿Se borran físicamente los registros de las bases de datos cuando el usuario los elimina, o se marcan como borrados? .....

5. Control de Aplicaciones

- ¿Todas las máquinas de la empresa tienen los mismos programas con las mismas versiones? ¿Existe un estándar de configuración de PC's a seguir? SI ---- NO ----
- ¿Usan alguna herramienta para copiar la configuración de las PC's? SI ---- NO ----
- ¿Existe un procedimiento para instalar las aplicaciones en las máquinas de los usuarios? SI ---- NO ----
- ¿Quién instala y administra? .....
- ¿Existen controles para realizar la instalación o actualización del software que se instala en las máquinas? SI ---- NO ----
- ¿Existe algún procedimiento para encontrar programas que no deberían estar en las máquinas de los usuarios, ya sea por problemas de licencias o virus? SI ---- NO ----
- ¿Existe un método a seguir? ¿Se usa algún producto para detectar estos programas? ¿Se hacen auditorías periódicas para verificar? SI ---- NO ----
- ¿Cómo se controla a los usuarios y las aplicaciones que bajan de la web?.....
- ¿Cómo controlan que éstas tengan las licencias correspondientes? ¿Se borran las versiones de prueba y demos cuando expiran? SI ---- NO ----
- ¿Se permiten los registros on line de las aplicaciones? SI ---- NO ----
- ¿Existen métodos para autorizar y registrar software? SI ---- NO ----
- ¿Cómo manejan las actualizaciones del software? …….....
- ¿Existe alguna forma de configurar las PC's de manera que no se pueda instalar software nuevo sin autorización del administrador? SI ---- NO ----

6. Mantenimiento de Aplicaciones.

- ¿Cómo se etiquetan y almacenan los instaladores de los programas o los drivers?
- ¿Se almacenan en disco duro, en CD, en cinta? .....
- ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte? SI ---- NO ----
- ¿Se controla el funcionamiento correcto de las aplicaciones? ¿Se hacen chequeos periódicos sobre el funcionamiento, la configuración, etc.? ¿Se generan alertas? SI ---- NO ----
- ¿Cómo se administran las emergencias?.....
- ¿Si se hacen cambios de emergencia, cómo se documenta?.....
- ¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basuras y provoquen la caída del sistema? SI ---- NO ----
- ¿Se revisan periódicamente los sistemas para eliminar los programas o servicios innecesarios? ¿Se buscan vulnerabilidades nuevas durante estas revisiones? SI ---- NO ----
- ¿Es automático el método de actualización de los antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus? SI ---- NO ----
- ¿Existe alguna aplicación de gestión para tomar decisiones de alto nivel gerencial? ¿Esta obtiene datos automáticamente de las bases de datos? SI ---- NO ----
- ¿Se hace un backup de la configuración de los sistemas antes de hacer algún cambio de manera de poder hacer un undo? SI ---- NO ----
- ¿Los cambios complejos en los archivos de configuración se hacen primero (a modo de prueba) en una copia de los archivos o se hacen directamente en la configuración original?.....
- ¿Se registran o documentan los cambios hechos a una configuración? SI ---- NO ----

7. Ciclo de Vida

- ¿Qué aplicaciones se desarrollaron en la empresa? ¿Una para cada área de la empresa?
- SI ---- NO ----
- ¿Qué metodología estándar usan para el desarrollo de sistemas?.....
- ¿De qué fases consta?.....

- ¿Qué mecanismos de seguridad manejan durante estas fases?.....

Análisis.

- ¿Cómo se expresan las necesidades del sistema?.....

Desarrollo.

- ¿Se hace un análisis de riesgos antes de empezar con el desarrollo? SI ---- NO ----
- ¿En caso de que haya participación de terceros, el código fuente queda en la empresa? ¿Dejan documentación? ¿Tiene alguna reglamentación para trabajar con terceros? SI ---- NO ----
- ¿Usan métricas durante el desarrollo? SI ---- NO ----
- ¿Les sirven? SI ---- NO ----
- ¿Se mantienen registros históricos de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento? SI ---- NO ----
- ¿Qué se guarda ?
  Sistema que afecta. ----
  Fecha de la modificación. ----
  Persona que realizó el cambio.----
  Descripción global de la modificación.----
  ¿Qué más? .....
- ¿En qué momento se definen los requisitos de seguridad de un sistema? ¿Es durante el desarrollo? SI ---- NO ----

Implementación.

- ¿En qué lenguajes se implementan los sistemas?
  …….....
- ¿Reúsan software? SI ---- NO ----
- ¿Qué medidas de seguridad toman durante la implementación?.....

Prueba.

- ¿Cómo se hace la prueba de los sistemas?.....
- ¿Se generan planes de prueba? SI ---- NO ----
- ¿Qué tipos de prueba se llevan a cabo?
  ¿De unidad? ----
  ¿De integración? ----
  ¿Por módulos? ----

¿Por sistema? ----

¿Se generan escenarios de prueba para el testeo? SI ---- NO ----

¿Se documentan las pruebas y sus resultados? SI ---- NO ----

- ¿Qué datos se guardan? .....
- ¿Cómo se realiza el control de cambios del sistema?.....

Instalación y Mantenimiento.

¿Qué metodología usan para el mantenimiento? …….....

Documentación.

- ¿Qué documentación generan de los desarrollos que hacen? ¿Incluyen? Generalidades del sistema, incluyendo fecha de implementación y analista programador responsable. SI ---- NO ----
- Documentación del sistema, incluyendo sus objetivos, diagramas general y de funciones y diseños de registros. SI ---- NO ----
- Documentación de los programas, incluyendo objetivos, diagrama de flujo y archivos de entrada y salida que utiliza. SI ---- NO ----
- Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores. SI ---- NO ----
- Manual del usuario. SI ---- NO ----
- Manual de características de seguridad. SI ---- NO ----
- Descripción, backup, plan de contingencia, descripción del usuario y del operador del sistema. SI ---- NO ----

Compra.

- ¿Qué medidas se toman antes de comprar un sistema?.....
- ¿Cómo es el análisis, que se hace ?.....
- ¿Existe documentación de los sistemas comprados, así como los vendedores y del soporte postventa? SI ---- NO ----

Anexo 6. Entrevista Evaluación Administración del CPD.

1. Administración CPD

- ¿Extraen un logístico sobre el volumen de correo transportado? SI ---- NO ----
- ¿Extraen un logístico sobre las conexiones de red levantadas? SI ---- NO ----
- ¿Extraen un logístico sobre los intentos de ingresos desde el exterior a la red interna? SI ---- NO ----
- ¿Extraen un logístico con las conexiones externas realizadas desde nuestra red?
- SI ---- NO ----
- ¿Obtienen un logístico sobre los downloads de archivos realizados y quién los realizó? SI ---- NO ----
- ¿Obtienen logísticos sobre conexiones realizadas en horarios no normales?
  SI ---- NO ----
- ¿Realizan un seguimiento de todos los archivos logísticos a fin de detectar cambios en las estadísticas obtenidas? SI ---- NO ----
- ¿Existe un programa que haga estas comparaciones? ¿Se usa? ¿Da buenos resultados? SI ---- NO ----
- ¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?
- SI ---- NO ----
- ¿Se entrena a los usuarios y administradores? SI ---- NO ----
- ¿Quién es el encargado? …..... ¿Por qué? …….....
- ¿Se tienen en cuenta los delitos no tecnológicos? SI ---- NO ----
- ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte? SI ---- NO ---- ¿Existe un tipo de feedback o buzón de sugerencia de cambios de los usuarios? SI ---- NO ----
- ¿Existe un Plan de Sistemas formal? (plan a corto plazo de actividades de CPD) SI ---- NO ----
- ¿Quién lo hace? .....
- ¿En base a qué estudios definen las cosas por hacer? .....
- ¿Existe un Plan Estratégico de Sistemas? (plan de largo plazo de proyectos)
- SI ---- NO ----
- ¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información? SI ---- NO ----

- ¿Existe una planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información? SI ---- NO ---

  Los procesos a realizar. ----

  Los controles que se efectúan. ----

  Los mecanismos de registros de problemas y hechos. ----

  Las relaciones con otras áreas. ----

  Los mecanismos de distribución de la información. ----
- ¿Existe documentación detallada sobre el equipamiento informático? SI ---- NO ----

  Distribución física de las instalaciones (identificación de PC's y equipos, y puestos de trabajo).

  Inventario de hardware y software de base. ----

  Número de serie de hardware. ----

  Número de licencia de software. ----

  Inventario de insumos. ----

  Diagramas topológicos de las redes. ----

  Ubicación de nodos. ----

  Trabajos de mantenimiento y entrada del personal externo. ----
- ¿Se tiene en cuenta tanto al centro de procesamiento de datos, redes departamentales, sucursales y al centro alternativo para contingencias? SI ---- NO ----
- ¿Se actualiza la lista de activos? SI ---- NO ----
- ¿Existe algún manual de seguridad, para el personal o para los usuarios?

  Plan de contingencia. ----

  Plan de continuidad. ----

  Plan de seguridad. ----
- Manual de Procedimientos del CPD. ----
- ¿Es automático el método de actualización de los antivirus? SI ---- NO ----
- ¿Cómo se etiquetan y almacenan los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en CD, en cinta? .....
- ¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basura y provoquen caídas del sistema? SI ---- NO ----
- ¿Todas estas tareas son realmente útiles? SI ---- NO ----
- ¿Se dan en la práctica? SI ---- NO ----

2. Responsabilidad del Equipo de Seguridad

- ¿Cómo se administran las emergencias? .....

- ¿Si se hacen cambios de emergencia, cómo se documenta? .....
- ¿Quién es el encargado de la seguridad? ¿Y de una política de seguridad y su administración?
- ....
- ¿Quién se encarga de administrar la estructura de seguridad una vez implementada?
- .....
- ¿Existe un solo responsable del centro de cómputo? SI ---- NO ----
- ¿Qué privilegios (o accesos) se le dan a las personas recién contratadas en el centro de cómputo ?.....
- ¿Cuál es la diferencia de permisos entre desarrolladores y los administradores?.....
- ¿Quién asigna los permisos a los distintos roles o grupos? .....
- ¿Quién es el encargado de informar a los ejecutivos de la empresa sobre la administración de seguridad, actividad de seguridad de la información y riesgos? ..... ¿Se realizan informes periódicos? SI — NO —
- ¿Son a pedido de alguien o a modo de auto evaluación? .....
- ¿Quién es el encargado de recomendar la separación de tareas y responsabilidades para las funciones de IT? .....
- ¿Quién es responsable de asegurar que los sistemas de seguridad física están en su lugar? .....
- ¿Existe en los empleados y altos ejecutivos una conciencia sobre su importancia de la seguridad? .....

3. Respaldos

- ¿Con qué frecuencia se hacen los backups? .....
- ¿Qué datos se almacenan? .....
  ¿Software base y configuración? SI ---- NO ----
- ¿Se hacen discos de inicio del Sistema Operativo? SI ---- NO ----
- ¿Se hace backups de la configuración de red? SI ---- NO ----
  Software aplicativo ----
  Parámetros del sistema ----
  Logs del sistema ----
  Datos ----
  - ¿Qué otra información se respalda?.....

4. Backups del hardware

- ¿Contratan un tercero que proporcione los recursos necesarios en caso de emergencia? SI ---- NO ----
- ¿Tienen equipos susceptibles de ser usados como equipos de emergencia en otro local de la empresa? SI ---- NO ----
- ¿Qué tipo de backup hacen: normales, incrementales, diferenciales?.....
- ¿En qué áreas utilizan los backups normales? .....
- ¿En qué áreas utilizan backups incrementales? .....
- ¿En qué áreas utilizan backups diferenciales? .....
- ¿En qué medios se almacenan?.....
- ¿Dónde se guardan estos medios y cómo?.....
- ¿Cada qué tiempo se hacen los backups: semanal, mensual, etc.?.....
- ¿Tienen herramientas de backup automáticas? SI ---- NO -----
- ¿Quién es el encargado de realizar los backups?.....
- ¿Existen procedimientos estandarizados para la realización de backups? SI ---- NO ----
- ¿Existe un plan de recuperación de backups? SI ---- NO ----
- ¿Los backups se almacenan dentro o fuera de la empresa? ¿Son estos lugares seguros? SI ---- NO ----
- ¿Hay documentación escrita sobre los backups, fechas, actualizaciones, etc.?

SI — NO—

- ¿Hay backups de las páginas web y de sus actualizaciones? SI ---- NO ----
- ¿Existen procedimientos automáticos para que la base de datos se recupere al estado anterior después de un error? SI ---- NO ----

Anexo 7. Entrevista Evaluación Plan de Seguridad.

1. Plan de Seguridad

- ¿Existe un Plan de contingencias? SI ---- NO ----
- ¿Quién lo desarrollo?.....
- ¿Ha habido alguna contingencia que justifique el desarrollo del plan de contingencias? SI ---- NO ----
- ¿Se desarrolló un previo análisis de riesgo antes de realizar el plan de contingencias? SI ---- NO ----
- ¿El plan de contingencias se desarrollo solo en base al área de cómputo, o se tuvieron en cuenta otras áreas de la empresa? SI ---- NO ---- ¿Cuáles? ..... ¿Por qué esas áreas?.....
- ¿El plan de contingencias incluye una Plan de recuperación de desastres? SI --- NO ---
- ¿El plan de contingencias incluye un Plan de reducción de riesgos? SI --- NO ---
- ¿Se definen las responsabilidades y funciones de las personas en el plan de contingencias? SI ---- NO ----
- ¿Existe entrenamiento para los responsables del plan de contingencias? ¿Y para los usuarios? SI ---- NO ----
- ¿Poseen las acciones defensivas en caso de violación interna o externa? (Ej. Desconectar los servidores, cerrar los accesos, rastrear al intruso, etc)? SI ---- NO ----
- ¿Hay algún tipo de mecanismo de reportes o historial, para el manejo de incidentes? SI — NO —
- ¿Documentan el plan de contingencias? ¿Contiene todos estos datos? SI ---- NO ----
  Objetivo del Plan. ----
  Modo de ejecución. ----
  Tiempo de duración. ----
  Costes estimados. -----
  Recursos necesarios. ----
  Evento a partir del cual se pondrá en marcha el plan. ----
  Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades. ----
- ¿Existe alguna copia del plan de contingencia fuera de la empresa? ¿Está protegida en caja de seguridad? ¿Cada cuanto se actualiza? ¿Se hacen pruebas del plan? SI --- NO --- ¿Con qué frecuencia?.....
- ¿Se mantiene actualizado de acuerdo a nuevos puestos y funciones, o amenazas? SI --- NO ---

2. CPD Alternativo

- ¿Se mantiene un centro de procesamiento alternativo? SI — NO —
- ¿Qué características tiene, en comparación con el CPD principal? …….....
- ¿Es propio o contratan un tercero que facilite el CPD? …..... En el segundo caso, ¿cómo es el contrato para este servicio?.....
- ¿Cómo se aseguran que este centro tenga las mismas condiciones de seguridad y calidad que las instalaciones del CPD principal?.....
- ¿Existe la posibilidad de poner el CPD alternativo en otra sucursal o en otro lado? SI --- NO --¿Por qué? .....
- ¿Si llega a haber un problema, en cuanto tiempo puede estar en funcionamiento este CPD alternativo? .....

3. Plan de Recuperación de Desastres.

- ¿Cuánto cuesta un plan de recuperación de desastres?..... ¿Tiene relación con la información a recuperar? SI ---- NO ----
- ¿O a cualquier costo se salva la información crítica? SI ---- NO ----
- ¿En el caso de que haya un plan, cada miembro del equipo tiene una responsabilidad asignada? ¿O la responsabilidad es del Departamento de Sistemas?.....
- ¿Se dividen las acciones correctivas en equipos de trabajo? SI ---- NO ---- ¿Cómo forman esos equipos? .....¿Dependen del desastre ocurrido? SI ---- NO ----
- ¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia? SI --- NO ----

4. Antes del desastre

- ¿Cuáles serían los datos críticos a proteger en la organización, en el momento de un desastre? .....
- ¿Cuáles serían los elementos de hardware y de software críticos a proteger en la organización, en el momento de un desastre? …….....
- ¿Cómo se ordenarían; según la importancia? SI ---- NO ----
- ¿Quién sería la responsable del plan de emergencias, de su implementación y puesta en práctica? ¿El jefe de sistemas? SI ---- NO ----
- En cada área que cubrirá el plan debe haber un líder del plan de contingencia SI ---- NO ---- ¿Quién sugiere, el jefe de cada área? SI ---- NO ---- ¿Alguien de más bajo rango? SI ---- NO ---- ¿Por qué? …….....

- ¿Existe un responsable de la información, en cada área de la empresa? SI ---- NO ---- ¿Conocen sus responsabilidades? SI ---- NO --- ¿Los responsables que figuran en la documentación, son los que ejercen realmente el papel de responsables de la información? SI ---- NO ---- ¿Qué funciones tiene que cumplir? …….....
- ¿Están identificados todos los sistemas de información y sus características? SI ---- NO ---- ¿Qué datos se almacenan de los sistemas?

  Nombre. ----

  Lenguaje. ----

  Departamento de la empresa que genera la información. ----

  Departamentos de la empresa que usan la información. ----

  Volumen de archivos con los que trabaja. ----

  Volumen de transacciones diarias, semanales y mensuales que maneja el sistema. ----

  Equipamiento necesario para un manejo óptimo del sistema. ----

  Las fechas en las que la información es necesidad con carácter de urgencia. ----

  Equipamiento mínimo necesario para que el sistema pueda seguir funcionando. ----

  Actividades a realizar para volver a contar con el sistema de información. ----
- ¿Existe un orden de importancia de los sistemas? SI ---- NO ----
- ¿Se mantiene un inventario de los equipos de cómputo? SI ---- NO ----

  Se debería incluir:

  Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges. ----

  Software: programas fuente, programas objeto, utilerías, programas de diagnóstico sistemas operativos, programas de comunicaciones. ----

  Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivos fuera de línea, backup, bases de datos, dueño designado de la información. ----

  Configuración de los equipos. ----

  Ubicación de los equipos y de los datos. ----

  Nivel de uso institucional de los equipos. ----
- ¿Existen pólizas de seguros para los equipos en caso de siniestros? SI ---- NO ----
- ¿Cómo son estos seguros? .....
- ¿Las PC’s o equipos se categorizan según su importancia o etiquetado de los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación ? SI ---- NO ----

- ¿Existe una relación de las PC's requeridas como mínimo para cada sistema permanente de la institución? ¿Está actualizada siempre? SI ---- NO ----
- ¿Existen procedimientos para realizar backup? SI ---- NO ----
- ¿Están incluidos en el plan de contingencia? SI ---- NO ----
- ¿Cuáles son las contingencias o problemas que pueden ocurrir?.....
- ¿Cuáles serían los peores problemas a los que se puede ver sometida la empresa?
  ¿Cuáles serian las peores contingencias? .....
  ¿Cuáles serían las más probables? .....
  ¿Cuáles son las que ocurren más a menudo? .....
  ¿Cuáles son las que no ocurren nunca? .....
- ¿Se pueden nombrar algunas funciones o servicios que funcionen como los niveles críticos de servicio para cada una de las contingencias? SI ---- NO ---- ¿Qué opinión tiene el jefe de cada área en cuanto a los niveles críticos de su área? .....
- ¿Cuáles son las prioridades de procesamiento que tendrán estas funciones o servicios críticos en caso de una emergencia? ….....
- ¿Qué costo tendría cada uno de los niveles críticos de servicio que se determinaron? …….....
- ¿Entrenan al personal de alguna manera ante un siniestro? SI ---- NO ----
- ¿Simulan siniestros para entrenar al personal? SI ---- NO ----

5. Durante el Desastre

- ¿Poseen un plan de emergencia (consiste de las acciones a llevar a cabo durante el siniestro)? SI ---- NO ----
- ¿Se tienen en cuenta los distintos escenarios posibles? SI ---- NO ----
  Se incluye:
  ¿Vías de salida? ----
  ¿Plan de evacuación del personal? ----
  ¿Plan de puesta a buen recaudo los activos? ----
  ¿Ubicación y señalización de los elementos contra incendio? ----
- ¿Existen funciones y equipos con funciones claramente definidas a ejecutar durante el siniestro? SI ---- NO ----

6. Después del desastre

- Evaluación de daños: ¿Se realizan las siguientes actividades después de que ha ocurrido algún desastre?

¿Se realiza la evaluación del alcance del daño que se ha producido? ----

¿Qué sistemas se están afectando? ----

¿Qué equipos han quedado no operativos? ----

¿Cuáles se pueden recuperar? ----

¿En cuánto tiempo? ----

- ¿Qué más se evalúa o debería evaluarse, según sus experiencias?.....
- ¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia? SI ---- NO ----
- ¿Para cada tipo de emergencia, ¿qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal? …….....
- ¿Se evalúan los desempeños de las personas, y del plan, luego de ocurrido el desastre? SI ---- NO ----
- ¿Se genera una lista de recomendaciones para minimizar los riesgos? SI ---- NO ----
- ¿Se evalúa el desempeño del personal durante el desastre? SI ---- NO ----

Anexo 8. Visión del Proyecto.

1. Introducción.

Propósito.

Empacadora del Pacífico "EDPACIF S.A" fue creada con la visión de satisfacer las necesidades de sus clientes y al mismo tiempo colaborar con el desarrollo socio-económico del sector de Coaque y Pedernales.

La empacadora inicio sus operaciones en el año 2001 dando como resultado su primera exportación en marzo del mismo año. "EDPACIF S.A" consiguió la certificación HACCP (Hazard Analysis and Critical Control Point) en el año 2002, lo que asegura un control de los puntos críticos en el procesamiento del camarón e incluye la trazabilidad del producto empacado en todas las operaciones de producción y comercialización. Está implementando actualmente el sistema de gestión BRC versión 6 (British Retail Consortium) es un sistema de seguridad alimentaria. Es una norma específica para la industria agroalimentaria, siendo sólo aplicable a compañías fabricantes o envasadoras de productos alimenticios.

Una de las fortalezas de "EDPACIF S.A" que perdura desde sus inicios hasta la actualidad es que sus productos sean una marca reconocida a nivel internacional por su calidad, inocuidad y legalidad, mediante el cumplimiento de los requisitos de sus clientes, lo cual ha generado una gran relación de confianza y el mantenimiento de clientes a largo plazo.

El propósito de esta aplicación surge como complemento a al trabajo de titulación denominado Auditoría de la Seguridad Informática de un Centro de Procesamiento de Datos y en la necesidad de contar con una herramienta web que permita documentar, dar seguimiento y facilitar la consulta del proceso de esta auditoría.

Alcance.

El aplicativo se basará en el estudio y análisis de la información recolectada en base a los siguientes componentes, mediante un banco de preguntas basadas en las métricas y actividades que sugiere el Marco de trabajo de Cobit.

- Seguridad Física.
- Seguridad Lógica.
- Seguridad de la Red.
- Seguridad de las Aplicaciones.
- Administración del CPD.
- Análisis del Plan de Seguridad.

2. Definiciones, Acrónimos y Abreviaciones.

Tabla 8.1.

Definiciones, acrónimos y abreviaturas.	
Abreviatura	**Definición**
COBIT	Objetivos de Control para la información y Tecnologías relacionadas.
RUP	Rational Unified Process.
TI	Tecnologías de Información.

Fuente: Muñoz, A. (2014)

3. Referencias.

Tabla 8.2.

Referencias.	
RUP	Rational Unified Process, metodología de software
COBIT	Objetivos de Control para la Información relacionadas

Fuente: Muñoz, A. (2014)

4. Posicionamiento.

Oportunidades de negocio.

Esta aplicación permitirá al auditor determinar si el Centro de procesamiento de Datos de la empresa EDPACIF S.A cumple con los estándares internacionales sobre seguridad de la información, especialmente relacionadas con el Marco de Trabajo de COBIT. De igual manera permitirá dar seguimiento al proceso de auditoría al ingresar la información de cada componente auditado.

Finalmente se constituirá en una herramienta de consulta para los usuarios que quieran saber cómo se la realiza y las actividades implicadas en la realización de una auditoría de seguridad de la información.

Sentencia que define el proceso.

Tabla 8.3.

Sentencia que define el proceso.	
El problema de:	Contar con una herramienta que permita dar seguimiento al proceso de auditoría y facilite su consulta.
Afecta a:	Auditor, Usuarios
El impacto asociado es:	No se cuenta con una aplicación para administrar y documentar la auditoría.
Una adecuada solución sería:	Automatizar el proceso, realizando una aplicación web que facilite la documentación y administración de la auditoría.

Fuente: Muñoz, A. (2014)

Secuencia que define la posición del Producto.

Tabla 8.4.

Secuencia que define la posición del producto	
Para:	Auditor (Tesista); Jefe Centro de Procesamiento de datos; Usuarios (Empleados, Estudiantes, Docentes)
Quiénes:	Realizan los procesos de control y administración de la seguridad del CPD. Quienes realizan las funciones de auditoría interna. Quienes quieran conocer las actividades de desarrollo de una auditoría.
Nombre del producto:	Aplicación web para la documentación y administración de la auditoría de seguridad de la información del CPD de Edpacif S.A.
Qué:	Almacena y presenta información de los procesos, análisis y resultados de la auditoría de la seguridad de la información del CPD.
No como:	El proceso se lleva manualmente y su documentación y seguimiento es demoroso y difícil de consultar.
El producto:	Facilitará la documentación y administración de la auditoría, permitirá ingresar los cuestionarios, la información colectada, debilidades, recomendaciones y estándares, facilitando su consulta de forma rápida mediante una interfaz sencilla y amigable.

Fuente: Muñoz, A. (2014)

Resumen de Stakeholders.

Tabla 8.5.

Resumen Stakeholders	
Descripción	**Responsabilidades**
Jefe CPD	Responsable de dar seguimiento al proyecto.
Auditor Sistemas	Responsable de la entrega de información para la auditoría, contacto con el auditor.

Fuente: Muñoz, A. (2014)

Resumen de usuarios.

Tabla 8.6.

Resumen Usuarios		
Nombre	**Descripción**	**Stakeholders**
Administrador	Podrá ingresar información a la aplicación.	Administrador
Usuarios Finales	Podrán consultar el proceso de auditoría.	Usuarios

Fuente: Muñoz, A. (2014)

5. Entorno de Usuarios.

- **El usuario Administrador**.- Es el responsable de la aplicación web, debe verificar la información e ingresar y mantener actualizada la información del proceso de auditoría de acuerdo al avance del mismo.
- **El usuario final**.- Podrá consultar los componentes, elementos, preguntas, respuestas, debilidades, efectos y recomendaciones de la auditoría de seguridad de la información del CPD.

Anexo 9. Especificación de Requerimientos.

1. Introducción.

El presente documento de especificación de requerimiento de software, surge como un conjunto de información necesaria que colabore al desarrollo, análisis y comprensión todos los requerimientos que el cliente desea, de la misma forma este constituye un informe útil, para que el cliente del producto final describa lo que él realmente desea obtener.

Se describirá en forma detallada la aplicación Web, las interfaces que contendrá, así como, los requerimientos y atributos del sistema.

2. Propósito.

- Definir de forma clara y precisa todas las funcionalidades y restricciones del sistema.
- Este documento será un canal de comunicación entre todos los involucrados.
- Este documento servirá como base para la construcción del sistema.

3. Alcance.

Desarrollar e implementar el sistema Web para la administración de la auditoría de seguridad de la información del CPD.

4. Objetivos del Proyecto:

- Desarrollo e implementación de una aplicación web.
- Permitir la gestión de la auditoría.
- Permitir el ingreso de información necesaria para la realización de la auditoría.
- Permitir registrar los resultados y el análisis de la auditoría.
- Permitir consultas de las actividades realizadas durante la auditoría.

5. Personal Involucrado.

Tabla 9.1.

Personal Involucrado.	
Nombre	Edmundo Arturo Muñoz Ramos
Rol	- Gestor del Proyecto. - Analista de Requerimientos. - Programador. - Diseñador de base de datos.
Categoría profesional	Analista – Programador.
Responsabilidades	-Análisis y especificaciones de requerimientos. - Diseño de la arquitectura del sistema.
Información de contacto	arturo_junior1707@yahoo.com

Fuente: Muñoz, A. (2014)

6. Resumen.

Este documento de especificación de requerimientos, está compuesto de la siguiente manera:

- Introducción: En esta sección se detalla los objetivos que tiene el Sistema.
- Descripción General: Describe la perspectiva general del producto a desarrollarse, como también de los sistemas, además las características del usuario y las limitaciones que podría tener.
- Requerimientos Específicos: Muestra todos los requerimientos que el usuario desea del producto final.

Anexo 10. Plan de desarrollo de software

1. Gestión del Proyecto.

Plan de Fases.

Inicio

Tabla 10.1.

Cronograma Fase Inicio	
Disciplinas /Artefactos	**Inicia**
Casos de uso del negocio y modelado	12 /04/2013
Casos de uso, especificaciones	13 /04/2013
Modelo de Análisis / Modelo de Datos	14/04/2013
Prototipos de Interfaz	15 /04/2013
Pruebas funcionales	16/04/2013
Gestión de Cambios y configuración	Permanente
Plan de desarrollo de software	12 al 28/04/2013

Fuente: Muñoz, A. (2014)

Fase Elaboración.

Tabla 10.2.

Cronograma Fase Elaboración	
Disciplinas /Artefactos	**Inicia**
Casos de uso del negocio y modelado	17 al 18 /04/2013
Casos de uso, especificaciones	19 al 20/04/2103
Modelo de Análisis / Modelo de Datos	21 al 22/04/2013
Prototipos de Interfaz	23 al 24/04/2013
Pruebas funcionales	25 al 26/04/2013
Gestión de Cambios y configuración	Permanente
Plan de desarrollo de software	12 al 28/04/2013

Fuente: Muñoz, A. (2014)

Fase de Construcción 1

Tabla 10.3.

Cronograma Fase Construcción 1	
Disciplinas /Artefactos	**Inicia**
Casos de uso primera iteración	
Ingresar Elementos (Gestión elementos)	02/05//2103
Ingresar Preguntas (Gestión Preguntas)	06/05/2013
Ingresar Respuestas (Gestión análisis)	11/05/2013
Cargar Tablas componentes	16/05/2013

Fuente: Muñoz, A. (2014)

Fase de Construcción 2

Tabla 10.4.

Cronograma Fase Construcción 2	
Disciplinas /Artefactos	**Inicia**
Casos de uso segunda iteración	
Eliminar Elementos (Gestión elementos)	21/05/2103
Eliminar Preguntas (Gestión entrevista)	24/05/2013
Eliminar Respuestas (Gestión Análisis)	27/05/2013
Editar / Consultar Elementos (Gestión Elementos)	01/06/2013
Editar / Consultar Preguntas (Gestión Entrevista)	04/06/2013
Editar / Respuestas (Gestión Análisis)	08/06/2013

Fuente: Muñoz, A. (2014)

Anexo 11. Arquitectura de Software.

1. Propósito.

El propósito del presente documento, provee una visión general para la arquitectura de la aplicación web.

Este documento proporciona una descripción de la arquitectura del sistema. Se realiza con el fin de documentar las decisiones de arquitectura.

2. Alcance.

Se muestra el diseño de la arquitectura. En cada una, se presentan los diagramas correspondientes como; modelo conceptual, diagrama de clases, casos de uso, diagramas de interacción, entre otros.

3. Definiciones.

Tabla 11.1.

Definiciones	
Paquetes	Agrupaciones de casos de uso y actores por funcionalidad que proveen.
Actor	Alguien o algo externo al sistema que interactúa con él.
Caso de Uso	Secuencia de acciones que el sistema realiza, la cual proporciona un resultado de valor observable.
Star UML	Se refiere a las herramientas que permiten realizar el modelado de los diagramas presentados en este documento.

Fuente: Muñoz, A. (2014)

4. Acrónimos y abreviaturas.

Tabla 11.2.

Acrónimos y abreviaturas	
ERS	Especificación de Requisitos de Software
RUP	Rational Unified Process
UML	Unified Modeling Language

Fuente: Muñoz, A. (2014)

5. Representación Arquitectural

El modelo propuesto por RUP para representar la arquitectura para el desarrollo de este proyecto de investigación, utiliza el siguiente conjunto de vistas:

- Vista de Casos de Uso: A cada uno se le hará una descripción en formato breve para enunciar su Escenario Principal de Éxito. Se utilizará el Diagrama de Casos de Uso en notación UML.

- Vista Lógica: Se realizará el Modelo Conceptual de la aplicación, que permita comprender el dominio del problema, utilizando la notación UML. Además, se desarrollará la primera versión del Diagrama de Clases de la aplicación para representar el dominio de la solución, utilizando también la notación UML y patrones.
- Vista de Implementación: Se explicará la estructura que describe el modelo de implementación de la aplicación, su composición en capas y cada uno de sus componentes.
- Vista de Despliegue: Se muestra la relación de la aplicación a desarrollar con el hardware requerido para el despliegue del sistema.
- Vista de Procesos: Se habla de los procesos (si existen).
- Vista de Datos: Describe los elementos principales del Modelo de Datos, brindando un panorama general de dicho modelo en términos de tablas, vistas, índices, etc. Se mostrará el Diagrama Entidad-Relación.

5.1. Vista Casos de uso.

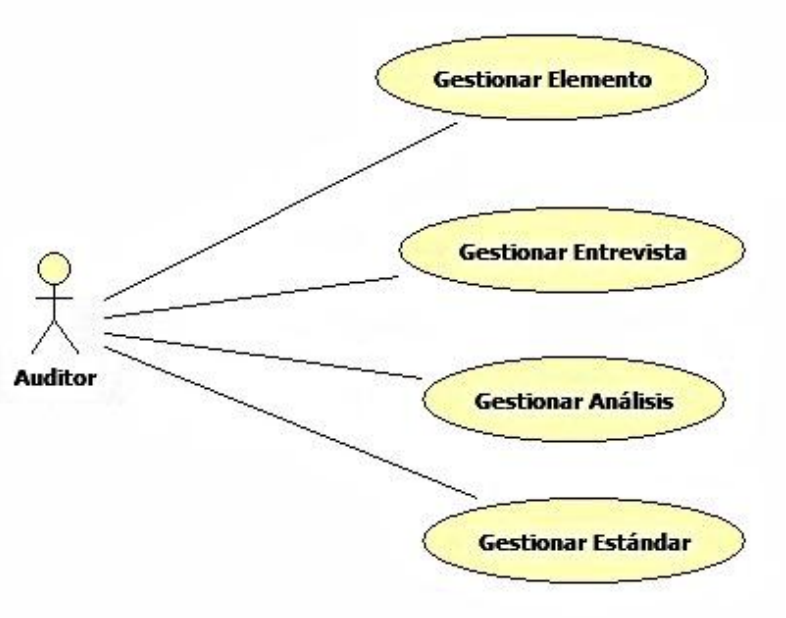


Figura 11.1. Casos de uso del negocio Auditor.
Fuente: Muñoz, A. (2014)

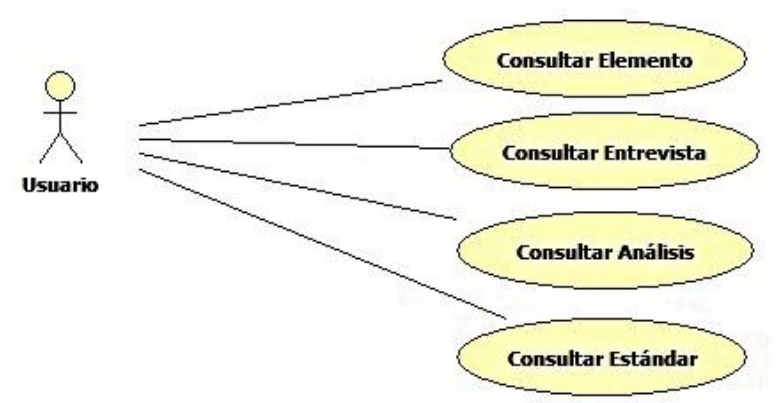


Figura 11.2. Caso de uso del negocio Usuario.
Fuente: Muñoz, A. (2014).

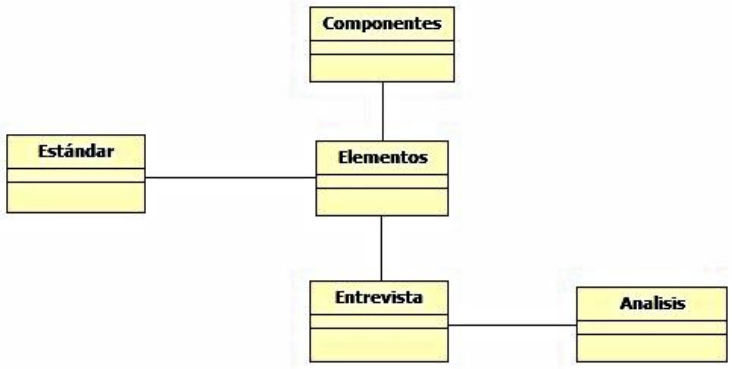


Figura 11.3. Modelo de dominio
Fuente: Muñoz, A. (2014)

Auditor (Administrador).

Es el encargado de realizar las funciones principales tales como ingresar, editar y eliminar información, de las diferentes tablas.

Los principales casos de uso son los que realiza el actor administrador, esto es Gestión de Elementos, Gestión Preguntas, Gestión Respuestas. Estos casos constituyen la base de la aplicación ya que son los encargados de cargar información a las diferentes tablas; información que posteriormente serán consultados por los actores usuarios.

- **Gestión Elementos**.- Este caso de uso permite al administrador ingresar, editar y eliminar información referente a los elementos que se deben revisar en una auditoría de seguridad de la información.
- **Gestión Entrevista**.- Este caso de uso permite al administrador ingresar, editar y eliminar las preguntas que son la base para obtener la información necesaria para

conocer si el CPD cumple con la normativa de Cobit para garantizar la seguridad de la información.

- **Gestión Análisis**.- Este caso de uso permite al administrador ingresar, editar y eliminar las respuestas y el análisis de las mismas para determinar sus debilidades, efectos y así poder emitir las recomendaciones para minimizar o eliminar estas debilidades.
- **Gestión Estándar**.- Este caso de uso permite ingresar información relacionada a los dominios del estándar Cobit, para así poder relacionarlo con la información obtenida.

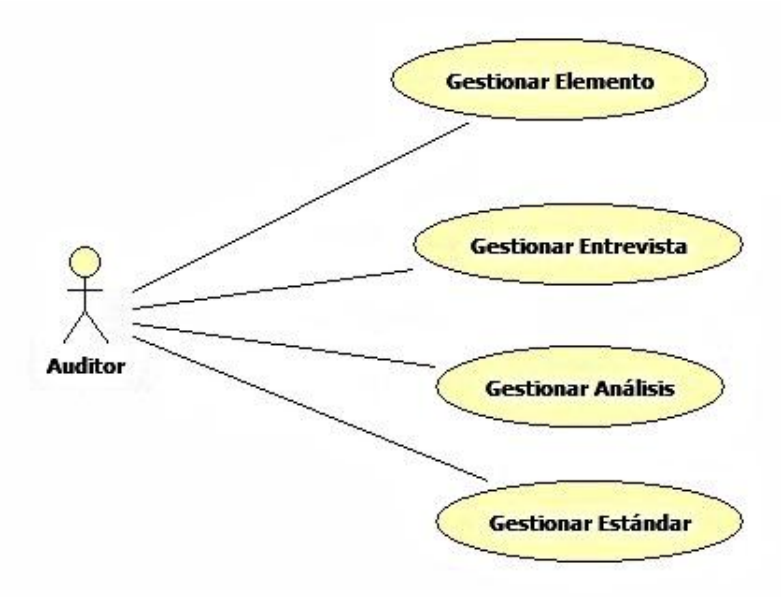


Figura 11.4. Casos de uso Administrador
Fuente: Muñoz, A. (2014)

Caso de uso Gestión Elemento.

La pantalla muestra una lista con los elementos introducidos en el sistema. Esta lista tiene los campos “Componente”, “Código”, “Nombre Elemento”, “Descripción”, “Fecha Elaboración” “Fecha Aplicación” y “Estado”.

1. El actor puede pulsar en cualquiera de los elementos y pulsar el botón “Editar” o “Borrar”.
2. Si pulsa el botón “Editar” se abrirá una pantalla donde podrá visualizar la información del elemento y modificarlo.

   Se abrirá una pantalla con la información ingresada del elemento, donde el actor puede corregir o completar la información del elemento.

   Una vez finalizado el cambio, se guardará el cambio pulsando el botón “Guardar”.
3. Si pulsa el botón “Borrar” el sistema, borrará el elemento seleccionado.

4. El actor puede pulsar el botón “Nuevo” para ingresar un nuevo elemento.
   Se abrirá una pantalla donde podrá introducir la información del elemento.
   Una vez finalizada la introducción de los datos si pulsa el botón “Guardar”, el elemento se almacenará en el sistema.
5. Para salir de Gestión Elementos presionar en el botón regreso.
6. Precondiciones
   El actor ha realizado correctamente el login en el sistema.
   El actor ha seleccionado “Gestión Elementos” de su interfaz gráfica.
   El actor ha ingresado el componente al que pertenece el elemento.

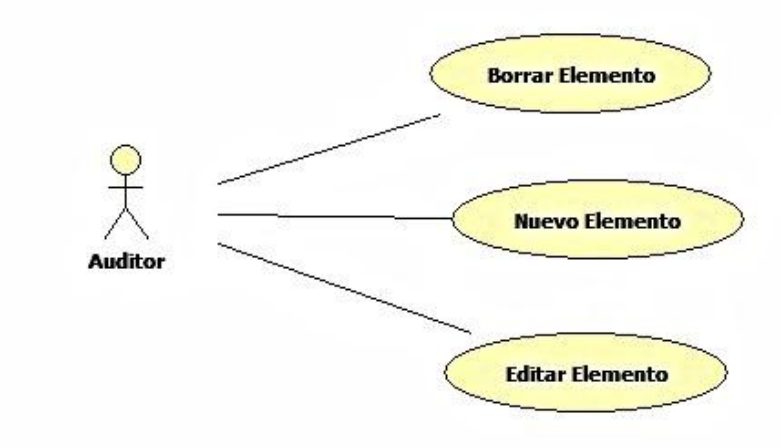


Figura 11.5. Casos de uso Gestión Elementos
Fuente: Muñoz, A. (2014)

Caso de uso: Gestión Entrevista.

1. Descripción: El caso de uso lo ejecuta el actor Auditor. Se utiliza para actualizar la tabla Preguntas que contiene información sobre los cuestionarios aplicados en la auditoría. Permite introducir las preguntas que se realizarán para recabar información de los elementos a auditar. Por otra parte permite revisar las preguntas ya ingresadas.
2. Flujo de Eventos
   La pantalla muestra una lista con los elementos introducidos en el sistema. Esta lista tiene los campos “Código”, “Nombre Pregunta”, “Número Elemento”, “Estado”.
   El actor puede pulsar en cualquiera de las preguntas y pulsar el botón “Editar” o “Borrar”.
   Si pulsa el botón “Editar” se abrirá una pantalla donde podrá visualizar la información de la pregunta y modificarla.
   Se abrirá una pantalla con la información ingresada del elemento, donde el actor puede corregir o completar la información de la pregunta.

Una vez finalizado el cambio, se guardará el cambio pulsando el botón “Guardar”.

Si pulsa el botón “Borrar” el sistema, borrará el elemento seleccionado.

3. El actor puede pulsar el botón “Nuevo” para ingresar una nueva pregunta.

   Se abrirá una pantalla donde podrá introducir la información de la pregunta.

   Una vez finalizada la introducción de los datos si pulsa el botón “Guardar”, la pregunta se almacenará en el sistema.
4. Para salir de Gestión Preguntas presionar en el botón regreso.
5. Precondiciones.

   El actor ha realizado correctamente el login en el sistema.

   El actor ha seleccionado “Gestión Preguntas” de su interfaz gráfica.

   El actor ha ingresado componentes y elementos.

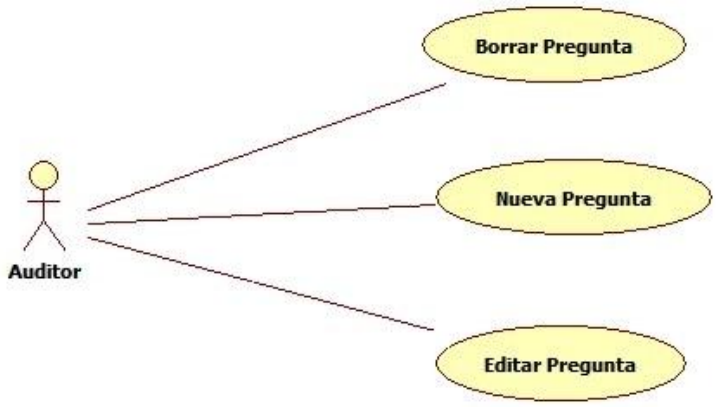


Figura 11.6. Casos de uso Gestión Entrevista
Fuente: Muñoz, A. (2014)

*Caso de uso: Gestión Análisis**.***

El caso de uso lo ejecuta el actor Auditor. Se utiliza para actualizar la tabla Respuestas que contiene información sobre las respuestas a los cuestionarios aplicados en la auditoría. Permite introducir las respuestas, debilidades, efectos y recomendaciones de cada elemento auditado. Por otra parte permite revisar las respuestas y el análisis de los registros ya ingresados.

Flujo de eventos.

1. La pantalla muestra una lista con las respuestas ingresadas en el sistema. Esta lista tiene los campos “Código Respuesta”, “Respuesta”, “Estándar”, “Debilidad”, “Efecto” y “Recomendación”.

2. El actor puede pulsar en cualquiera de las respuestas y pulsar el botón “Editar” o “Borrar”.
3. El actor puede pulsar el botón “Editar” para corregir o aumentar información de la respuesta.

   Se abrirá una pantalla con la información ingresada de la respuesta, donde el actor puede corregir o completar la información.

   Una vez finalizado el cambio, se guardará el cambio pulsando el botón “Guardar”.
4. Si pulsa el botón “Borrar” el sistema, tras pedir la confirmación, la respuesta seleccionada.
5. El actor puede pulsar el botón “Nuevo” para ingresar una nueva respuesta.

   Se abrirá una pantalla donde podrá introducir la información de la nueva respuesta.

   Una vez finalizada la introducción de los datos si pulsa el botón “Guardar”, el registro se almacenará en el sistema.
6. Precondiciones

   El actor ha realizado correctamente el login en el sistema.

   El actor ha seleccionado el botón “Respuestas” de su interfaz gráfica.

   El actor ha ingresado Preguntas y Estándar previamente.

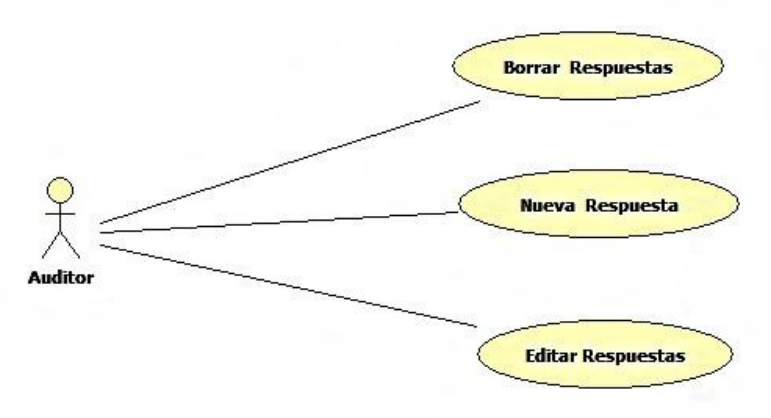


Figura 11.7. Casos de uso Gestión Análisis
Fuente: Muñoz, A. (2014)

Usuario.

Usuarios (Ejecutivos, Jefe de Sistemas, otros usuarios).- estos usuarios tienen acceso solo a consultas.

Caso de uso: Gestión Consultas.

El caso de uso lo ejecuta el actor Usuario. Se utiliza para consultar la información de la auditoría, referente a elementos auditados, preguntas realizadas en las entrevistas por cada

elemento, las respuestas a los cuestionarios aplicados en la auditoría y las debilidades encontradas, efectos que estas ocasionan y las recomendaciones para mitigar los efectos de cada debilidad detectada.

Este caso de uso permite a los usuarios obtener información relacionada con la auditoría de seguridad de la información del Centro de Procesamiento de Datos (CPD); el usuario puede, consultar información referente a los diferentes componentes, elementos, preguntas utilizadas en el levantamiento de la información, la información recopilada, el análisis que incluye debilidades, efectos y recomendaciones, basado en el estándar Cobit.

Flujo de eventos

1. En cada pantalla del aplicativo el usuario puede seleccionar el componente que desea Consultar.
2. La interfaz muestra información del componente y un submenú con los nombres de los elementos que lo conforman.
3. El actor usuario puede seleccionar el elemento que desea consultar.
4. La interfaz muestra la información del elemento y un submenú donde puede seleccionar consultar Preguntas, consultar Respuestas, regresar a la interfaz anterior o regresar a la página principal.

   Si escogió la opción Preguntas el aplicativo presenta un listado de las preguntas relacionadas con el componente y elemento seleccionados, para salir debe presionar el botón “Regresar”.

   El mismo procedimiento ocurre si escoge la opción Respuestas.
5. Precondiciones

   El actor ha seleccionado por lo menos un componente, un elemento y una opción.

   El actor auditor ha ingresado toda la información en las tablas del aplicativo.

.

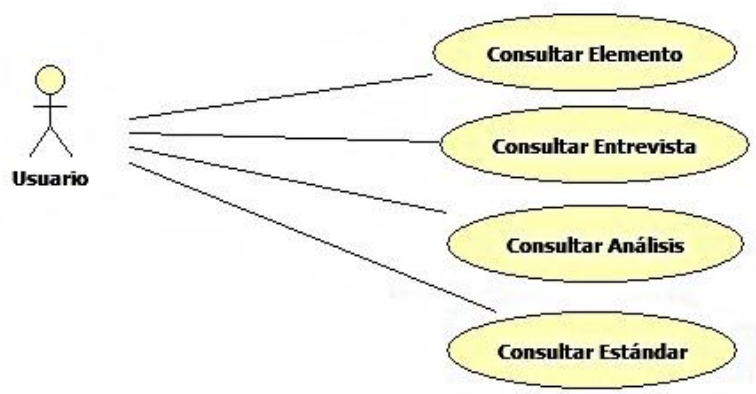


Figura 11.8. Casos de uso Usuario
Fuente: Muñoz, A. (2014)

5.2. Vista Lógica.

5.2.1. Diagrama de Clases.

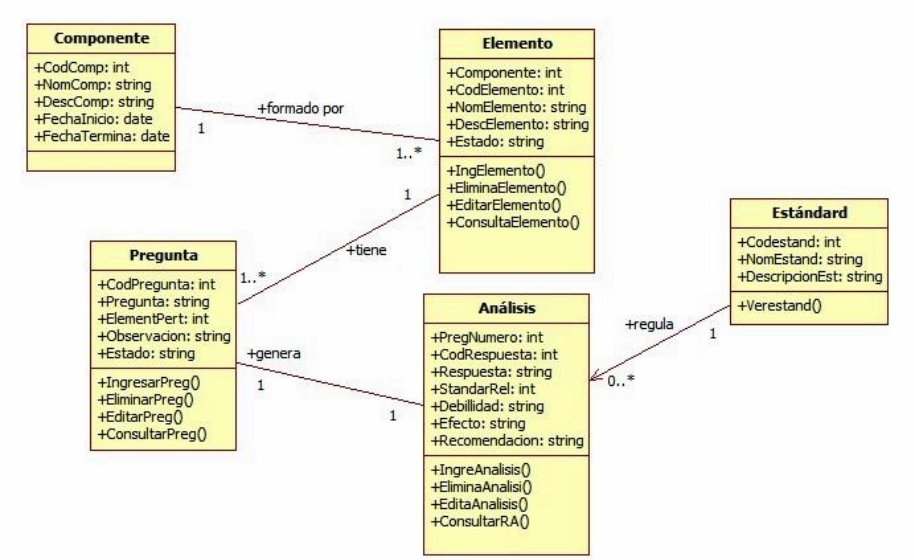


Figura 11.9. Diagrama de Clases.
Fuente: Muñoz, A. (2014)

- Componente.- Esta clase contiene información de los componentes a auditar.
- Elemento.- Esta clase contiene los elementos por cada componente que deben ser revisados en la auditoría.
- Pregunta.- Esta clase guarda las preguntas de las entrevistas, cada pregunta está relacionada con un elemento y con el estándar Cobit. También permite guardar su estado (elaborada, aplicada, terminado) y alguna observación relacionada a esa pregunta.
- Análisis.- Esta clase almacena la información recopilada en las encuestas y una vez analizadas también guarda las debilidades encontradas, los efectos de esas debilidades y las recomendaciones respectivas.
- Estándar.- Esta clase contiene información de los dominios de Cobit.

5.2.2. Diagrama de Datos.

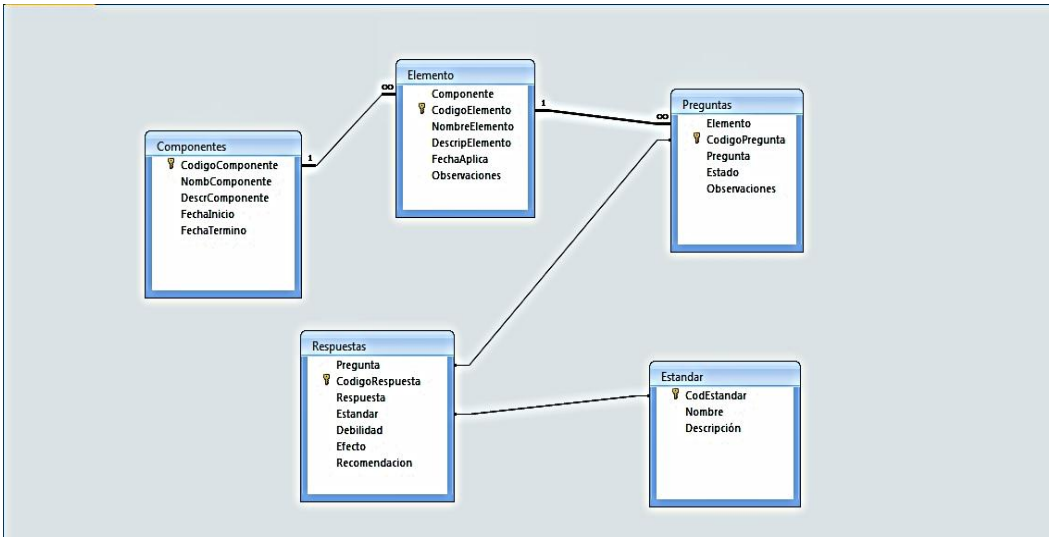


Figura 11.10. Diagrama de Clases.
Fuente: Muñoz, A. (2014)

5.2.3. Diagrama de Secuencia.

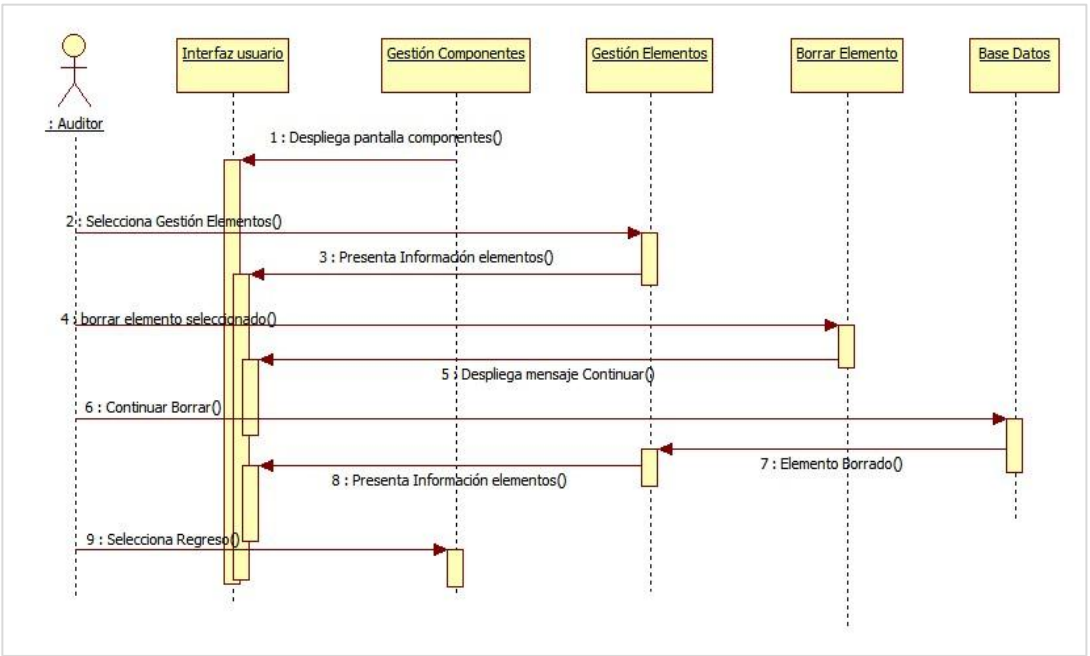


Figura 11.11. Diagrama de Secuencia Borra Elemento de Caso de Uso Gestión Elemento
Fuente: Muñoz, A. (2014)

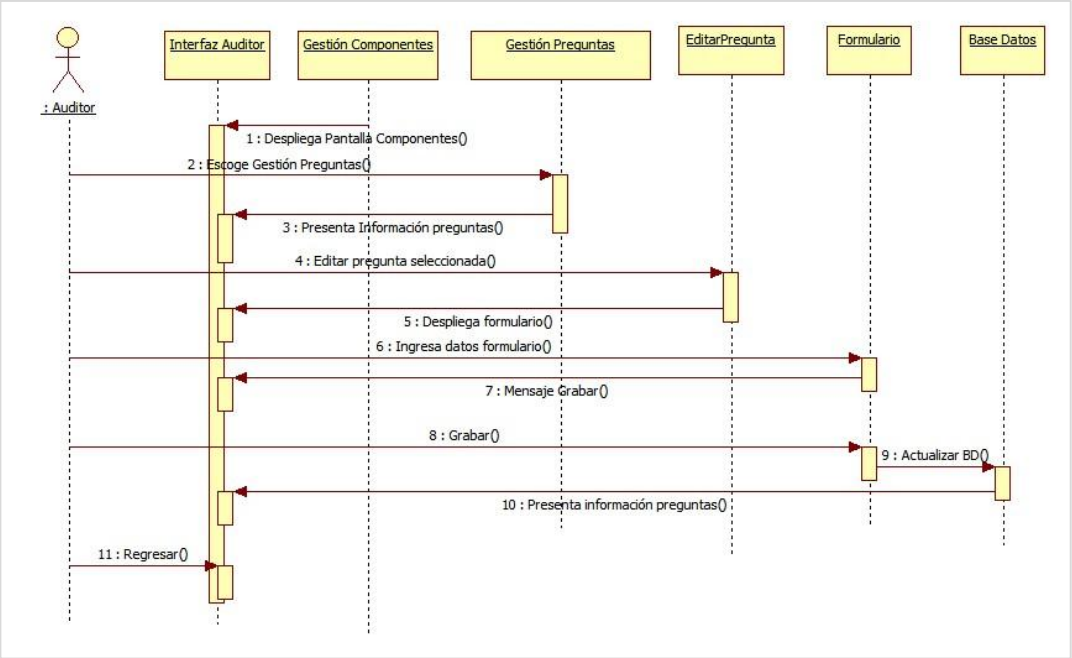


Figura 11.12. Diagrama Secuencia Pregunta de Caso de Uso Gestión Entrevista

Fuente: Muñoz, A. (2014)

.

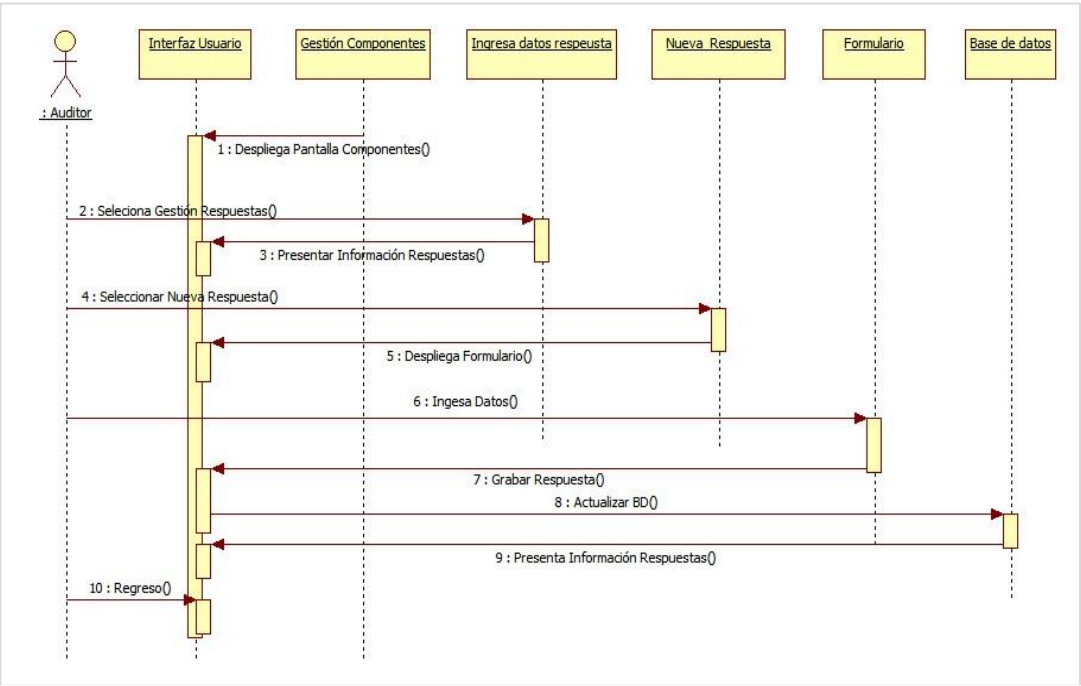


Figura 11.13. Diagrama de Secuencia Nueva Respuesta de Caso de Uso Gestión Análisis
Fuente: Muñoz, A. (2014)

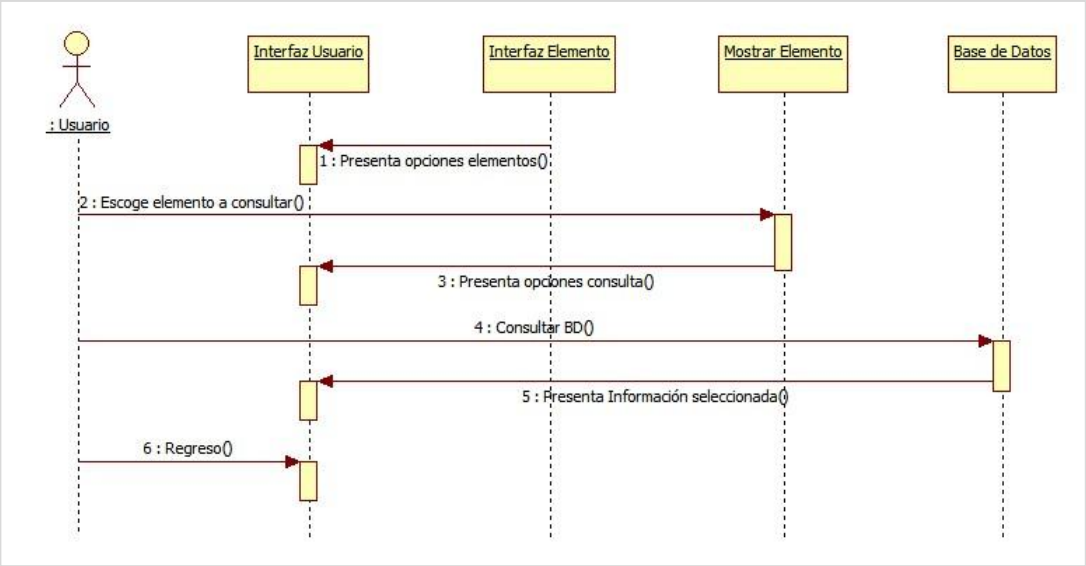


Figura 11.14. Diagrama de Secuencia Consulta Preguntas Gestión Consulta.
Fuente: Muñoz, A. (2014)

5.2.4. Diagrama de Colaboración.

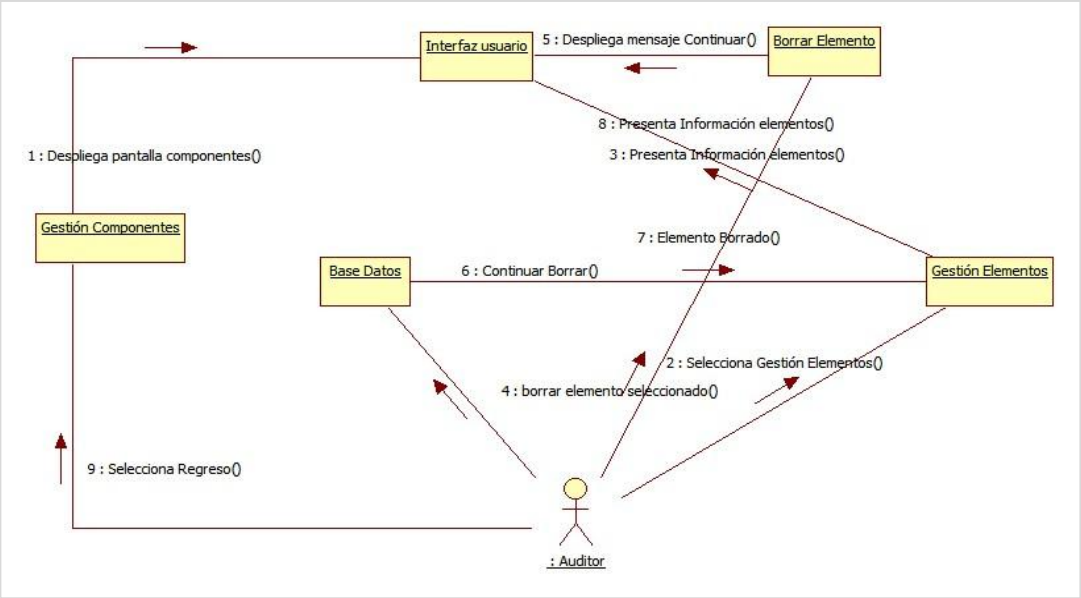


Figura 11.15. Diagrama de Colaboración Gestión Elemento.
Fuente: Muñoz, A. (2014)

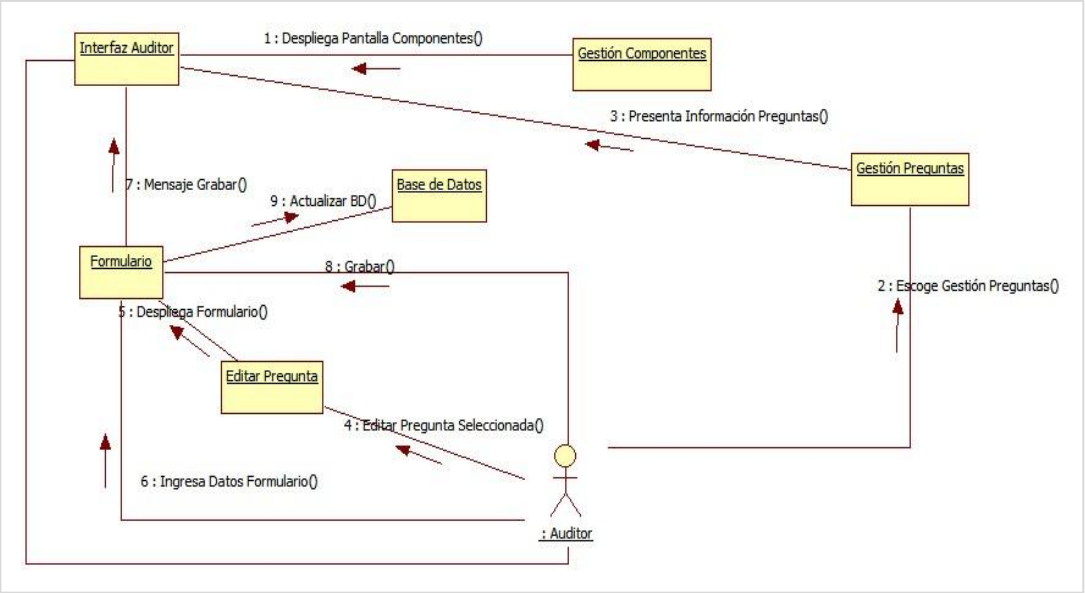


Figura 11.16. Diagrama de Colaboración Gestión Entrevista
Fuente: Muñoz, A. (2014)

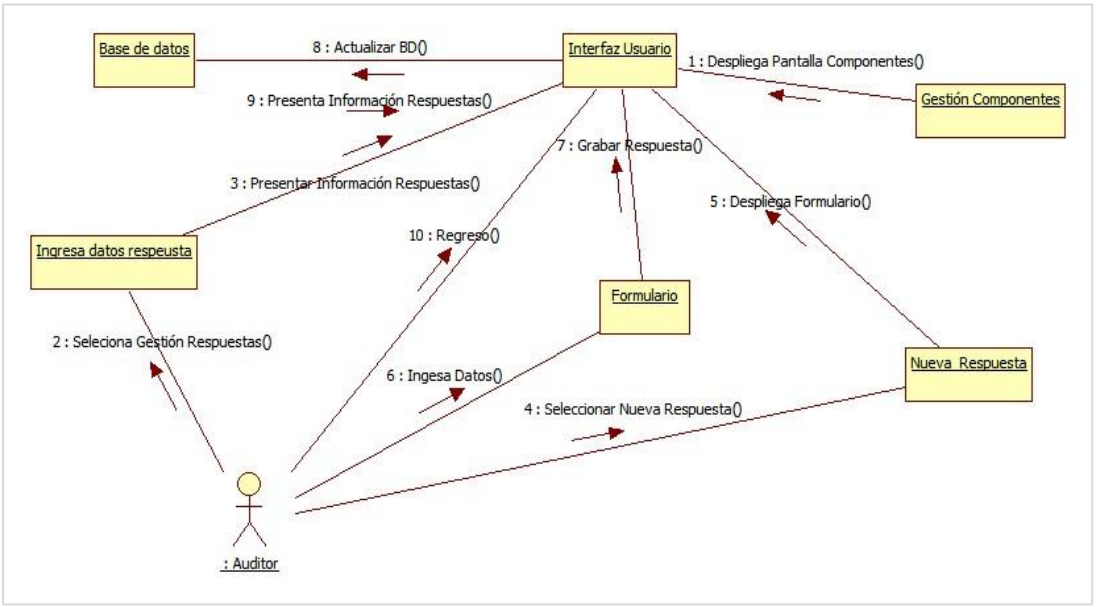


Figura 11.17. Diagrama de Colaboración Gestión Análisis
Fuente: Muñoz, A. (2014)

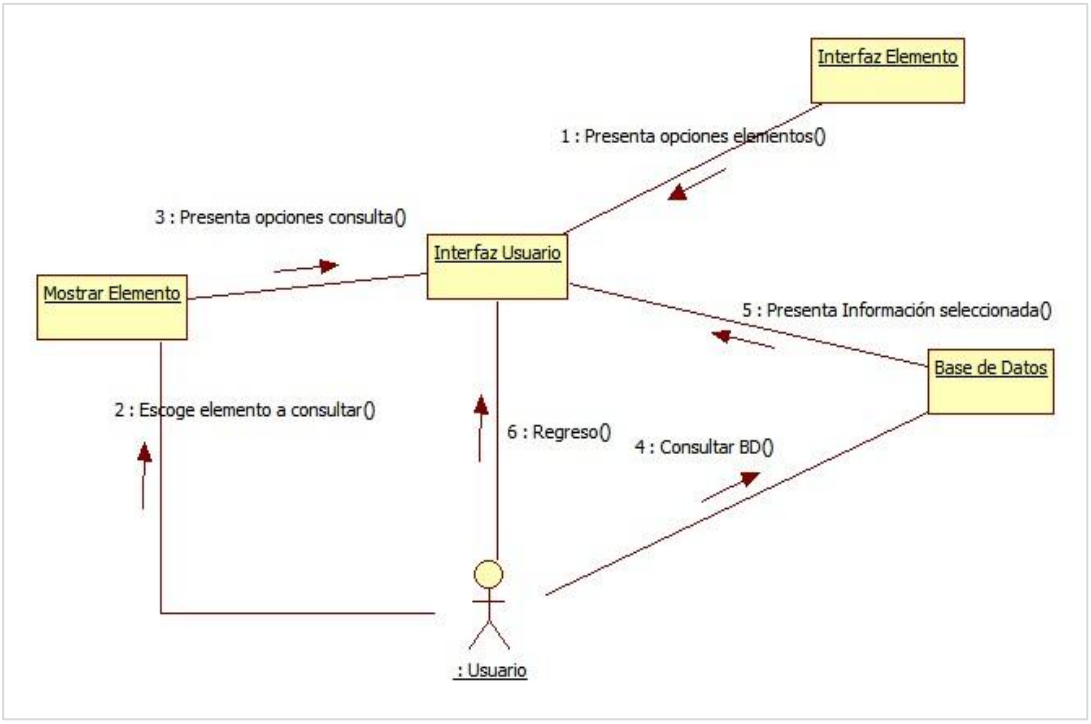


Figura 11.18. Diagrama de Colaboración Gestión Consulta.
Fuente: Muñoz, A. (2014)

5.2.5. Diagrama de Estado.

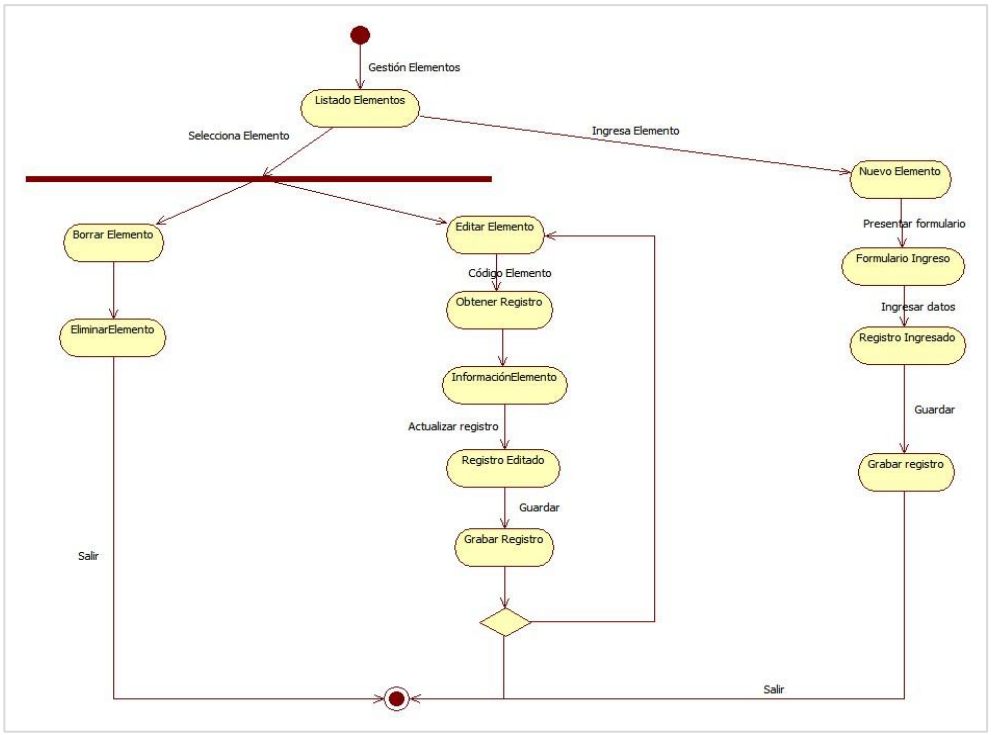


Figura 11.19. Diagrama de Estado Gestión Elemento.

Fuente: Muñoz, A. (2014)

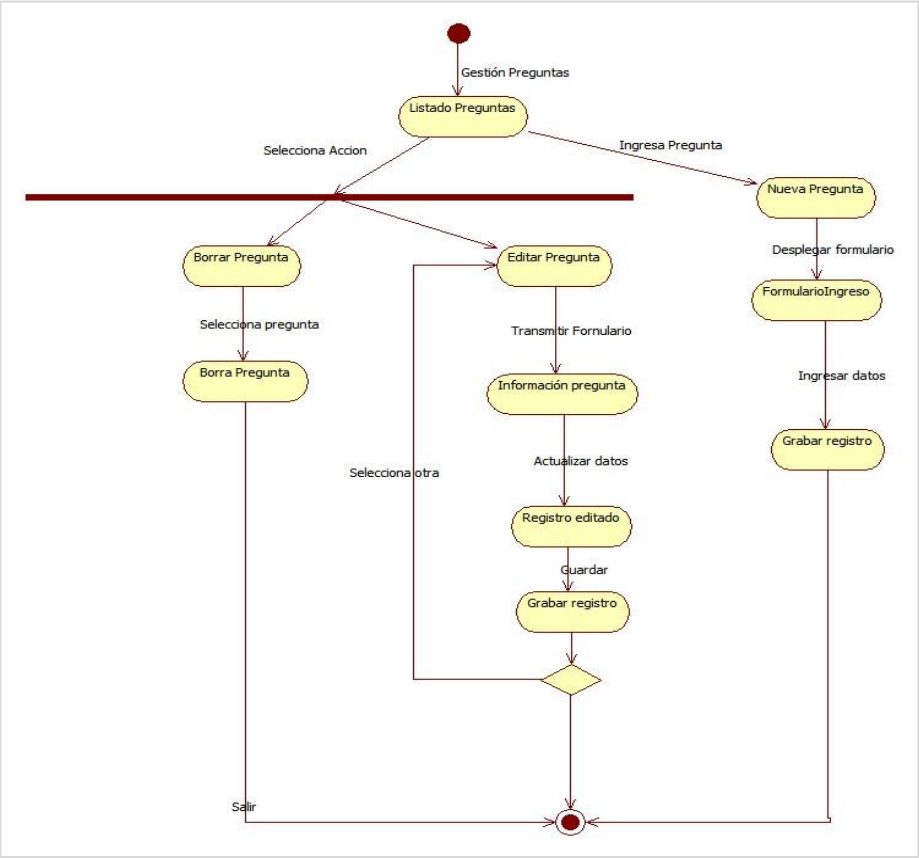


Figura 11.20. Diagrama de Estado Gestión Análisis
Fuente: Muñoz, A. (2014)

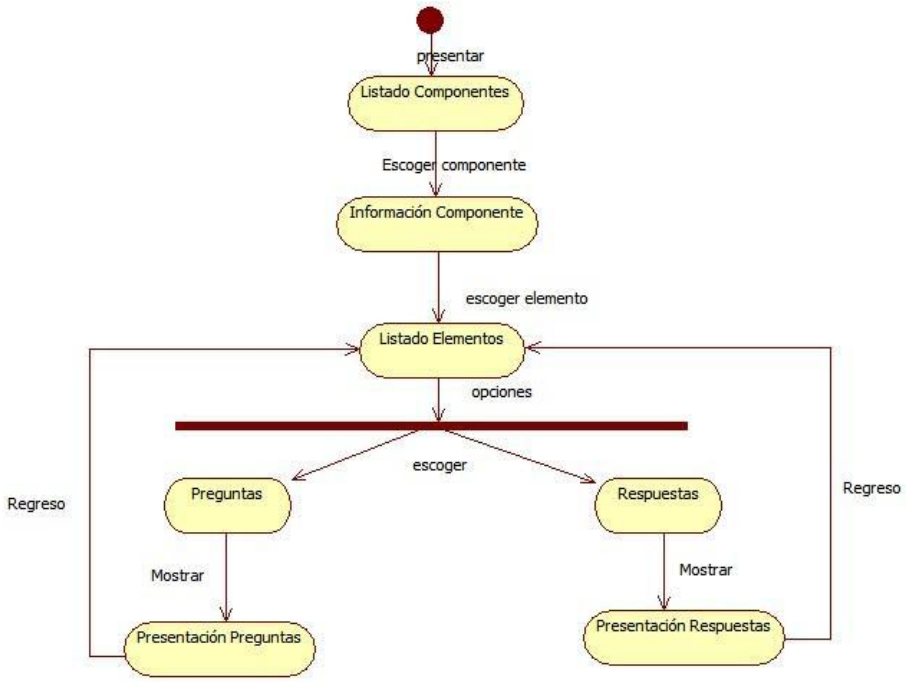


Figura 11.21. Diagrama de Estado Gestión Consulta.
Fuente: Muñoz, A. (2014)

5.2.6. Implementación.

.

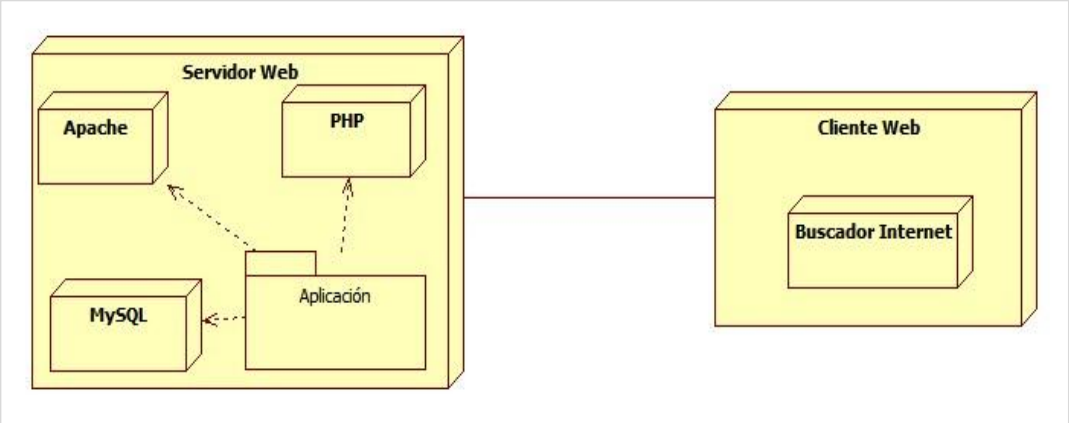


Figura 11.22. Diagrama Implementación
Fuente: Muñoz, A. (2014)

5.2.7. Prototipos de Interfaz de Usuario.

.

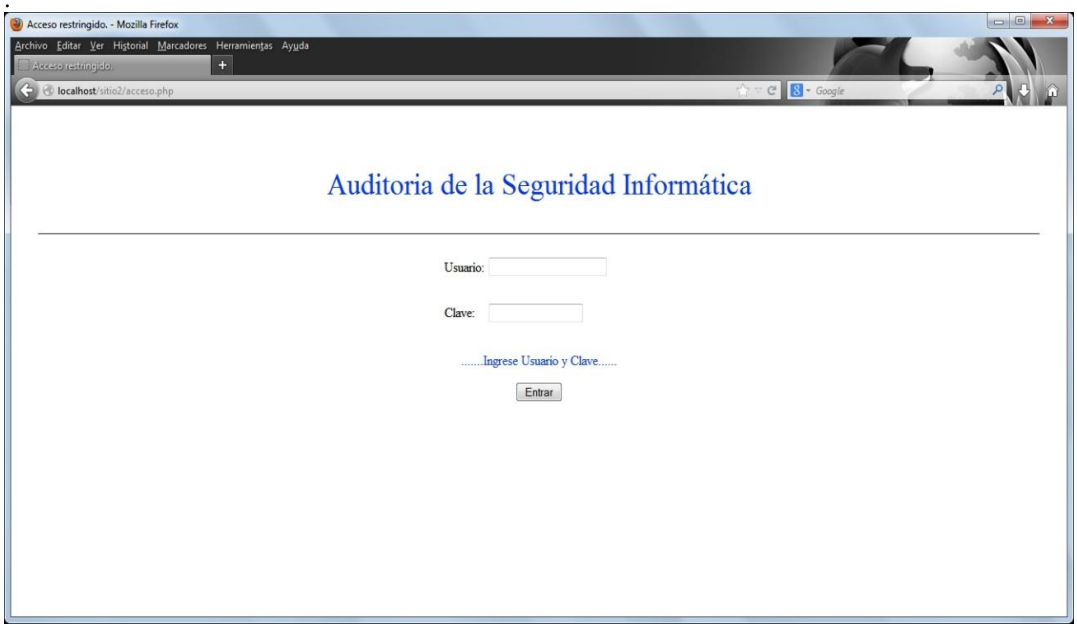
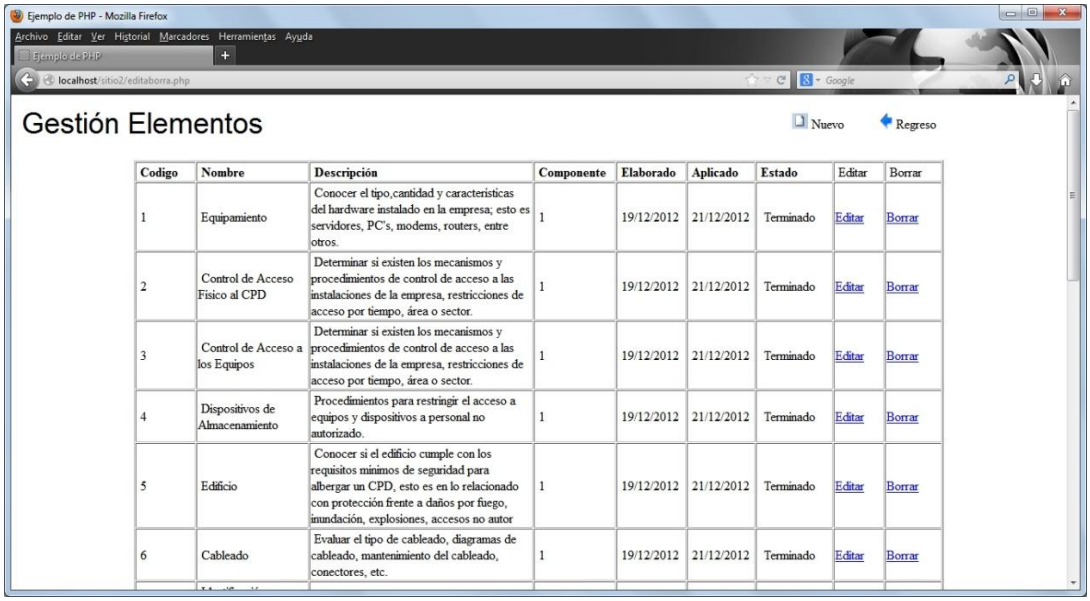
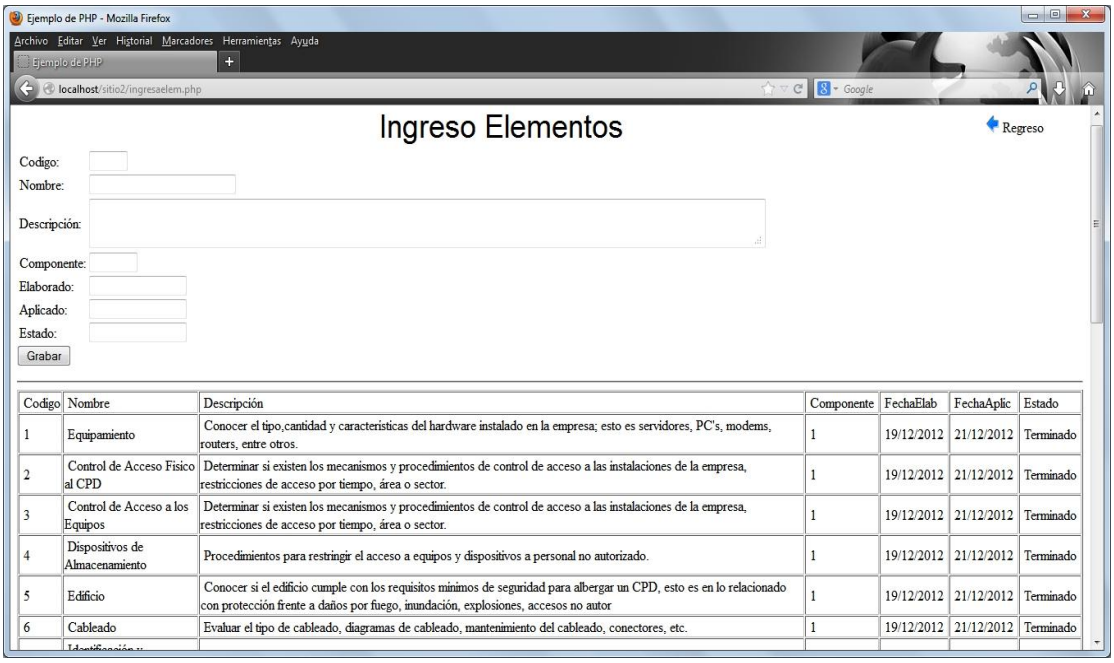


Figura. 11.23. Prototipo Interfaz Acceso
Fuente: Muñoz, A. (2014)



Codigo	Nombre	Descripción	Componente	Elaborado	Aplicado	Estado	Editar	Borrar
1	Equipamiento	Conocer el tipo,cantidad y caracteristicas del hardware instalado en la empresa; esto es servidores, PC's, modems, routers, entre otros.	1	19/12/2012	21/12/2012	Terminado	Editar	Borrar
2	Control de Acceso Fisico al CPD	Determinar si existen los mecanismos y procedimientos de control de acceso a las instalaciones de la empresa, restricciones de acceso por tiempo, área o sector.	1	19/12/2012	21/12/2012	Terminado	Editar	Borrar
3	Control de Acceso a los Equipos	Determinar si existen los mecanismos y procedimientos de control de acceso a las instalaciones de la empresa, restricciones de acceso por tiempo, área o sector.	1	19/12/2012	21/12/2012	Terminado	Editar	Borrar
4	Dispositivos de Almacenamiento	Procedimientos para restringir el acceso a equipos y dispositivos a personal no autorizado.	1	19/12/2012	21/12/2012	Terminado	Editar	Borrar
5	Edificio	Conocer si el edificio cumple con los requisitos minimos de seguridad para albergar un CPD, esto es en lo relacionado con protección frente a daños por fuego, inundación, explosiones, accesos no autor	1	19/12/2012	21/12/2012	Terminado	Editar	Borrar
6	Cableado	Evaluar el tipo de cableado, diagramas de cableado, mantenimiento del cableado, conectores, etc.	1	19/12/2012	21/12/2012	Terminado	Editar	Borrar

Figura 11.24. Prototipo Interfaz Gestión Elementos.
Fuente: Muñoz, A. (2014)



Codigo	Nombre	Descripción	Componente	FechaElab	FechaAplic	Estado
1	Equipamiento	Conocer el tipo,cantidad y caracteristicas del hardware instalado en la empresa; esto es servidores, PC's, modems, routers, entre otros.	1	19/12/2012	21/12/2012	Terminado
2	Control de Acceso Fisico al CPD	Determinar si existen los mecanismos y procedimientos de control de acceso a las instalaciones de la empresa, restricciones de acceso por tiempo, área o sector.	1	19/12/2012	21/12/2012	Terminado
3	Control de Acceso a los Equipos	Determinar si existen los mecanismos y procedimientos de control de acceso a las instalaciones de la empresa, restricciones de acceso por tiempo, área o sector.	1	19/12/2012	21/12/2012	Terminado
4	Dispositivos de Almacenamiento	Procedimientos para restringir el acceso a equipos y dispositivos a personal no autorizado.	1	19/12/2012	21/12/2012	Terminado
5	Edificio	Conocer si el edificio cumple con los requisitos minimos de seguridad para albergar un CPD, esto es en lo relacionado con protección frente a daños por fuego, inundación, explosiones, accesos no autor	1	19/12/2012	21/12/2012	Terminado
6	Cableado	Evaluar el tipo de cableado, diagramas de cableado, mantenimiento del cableado, conectores, etc.	1	19/12/2012	21/12/2012	Terminado

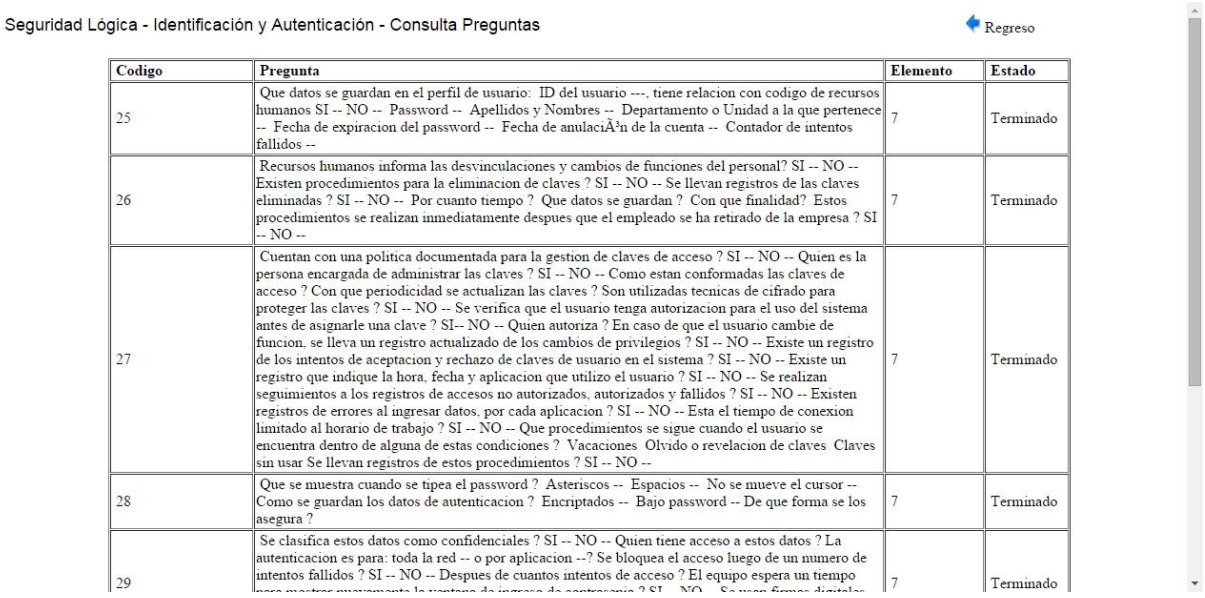
Figura 11.25. Interfaz Ingreso.
Fuente: Muñoz, A. (2014)

Anexo 12. Construcción

Módulo Administrador

Figura: 12.1. Pantalla Módulo Administrador
Fuente: Muñoz, A. (2014)

Módulo Consultas


Seguridad Lógica - Identificación y Autenticación - Consulta Preguntas

Regreso

Codigo	Pregunta	Elemento	Estado
25	Que datos se guardan en el perfil de usuario: ID del usuario ---, tiene relacion con codigo de recursos humanos SI -- NO -- Password -- Apellidos y Nombres -- Departamento o Unidad a la que pertenece -- Fecha de expiracion del password -- Fecha de anulaciÃ³n de la cuenta -- Contador de intentos fallidos --	7	Terminado
26	Recursos humanos informa las desvinculaciones y cambios de funciones del personal? SI -- NO -- Existen procedimientos para la eliminacion de claves ? SI -- NO -- Se llevan registros de las claves eliminadas ? SI -- NO -- Por cuanto tiempo ? Que datos se guardan ? Con que finalidad? Estos procedimientos se realizan inmediatamente despues que el empleado se ha retirado de la empresa ? SI -- NO --	7	Terminado
27	Cuentan con una politica documentada para la gestion de claves de acceso ? SI -- NO -- Quien es la persona encargada de administrar las claves ? SI -- NO -- Como estan conformadas las claves de acceso ? Con que periodicidad se actualizan las claves ? Son utilizadas tecnicas de cifrado para proteger las claves ? SI -- NO -- Se verifica que el usuario tenga autorizacion para el uso del sistema antes de asignarle una clave ? SI-- NO -- Quien autoriza ? En caso de que el usuario cambie de funcion, se lleva un registro actualizado de los cambios de privilegios ? SI -- NO -- Existe un registro de los intentos de aceptacion y rechazo de claves de usuario en el sistema ? SI -- NO -- Existe un registro que indique la hora, fecha y aplicacion que utilizo el usuario ? SI -- NO -- Se realizan seguimientos a los registros de accesos no autorizados, autorizados y fallidos ? SI -- NO -- Existen registros de errores al ingresar datos, por cada aplicacion ? SI -- NO -- Esta el tiempo de conexion limitado al horario de trabajo ? SI -- NO -- Que procedimientos se sigue cuando el usuario se encuentra dentro de alguna de estas condiciones ? Vacaciones Olvido o revelacion de claves Claves sin usar Se llevan registros de estos procedimientos ? SI -- NO --	7	Terminado
28	Que se muestra cuando se tipea el password ? Asteriscos -- Espacios -- No se mueve el cursor -- Como se guardan los datos de autenticacion ? Encriptados -- Bajo password -- De que forma se los asegura ?	7	Terminado
29	Se clasifica estos datos como confidenciales ? SI -- NO -- Quien tiene acceso a estos datos ? La autenticacion es para: toda la red -- o por aplicacion --? Se bloquea el acceso luego de un numero de intentos fallidos ? SI -- NO -- Despues de cuantos intentos de acceso ? El equipo espera un tiempo para mostrar nuevamente la ventana de ingreso de contrasena ? SI -- NO -- Se usan firmas digitales	7	Terminado

Figura: 12.2. Consulta Preguntas.
Fuente: Muñoz, A. (2014)

Codigo	Respuesta	Elemento	Pregunta	Estandar	Debilidad	Efecto	Recomendación
25	Los datos que se guardan en el perfil de usuario son: ID del usuario que tiene relacion con codigo de recursos humanos Password Apellidos y Nombres Departamento o Unidad a la que pertenece Fecha de expiracion del password	7	25	DS5	No se encontraron debilidades significativas	No aplica	No aplica
26	Recursos humanos informa las desvinculaciones y cambios de funciones del personal, existen pocedimientos para la eliminacion de claves,se llevan registros de las claves eliminadas, los mismos que se almacenan con la finalidad evitar repetir nombres de usuario y saber hasta que fecha el usuario accedio al sistema. Estos procedimientos se realizan inmediatamente despues que el empleado se ha retirado de la empresa.	7	26	DS5	No se encontraron debilidades significativas	No aplica	No aplica
	Cuentan con una politica documentada para la gestion de claves de acceso, la administracion de las claves es responsabilidad del personal de sistemas. Las claves de acceso deben estar conformadas por letras y numeros, minimo 4 caracteres, maximo 8 caracteres,se deben cambiar o actualizar cada tres meses. Para proteger las claves se utilizan tecnicas de cifrado, para la asignacion de claves se verifica que el usuario tenga la autorizacion del jefe inmediato del area donde trabaja el usuario.				No se cuenta con una politica documentada para la gestion de claves de acceso, esto se lo realiza basado en la experiencia del administrador de sistemas. No existe registro de los intentos	Al no existir una politica documentada para la gestion de claves se puede facilitar : adivinar o descubrir la clave mediante alguna tecnica de ingenieria social, lo que permitiria a una persona no autorizada acceso a recursos de informacion de uso	Documentar adecuadamente la politica de la empresa en cuanto a la gestion de claves de acceso determinando las medidas de gestion y proteccion de contrasenias, normas para proteger las contrasenias, normas para elegir contrasenias. Mantener un registro

Figura: 12.3. Consulta Respuesta.
Fuente: Muñoz, A. (2014)

- Consulta Cobit 4.1 -

Nombre	Descripción
AI1	Evaluar el plan de seguridad de la empresa con la finalidad de detectar debilidades y los posibles efectos en la seguridad, para de esta forma desarrollar sugerencias que permitan minimizar estos efectos para garantizar la continuidad del servicio.
AI2	Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseno de las aplicaciones, la inclusion apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuracion en si de acuerdo a los estandares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas
AI3	Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnologica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnologicas convenidas y la disposicion del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnologico continuo para las aplicaciones del negocio.
AI4	El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generacion de documentacion y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operacion correctos de las aplicaciones y la infraestructura.
AI5	Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definicion y ejecucion de los procedimientos de adquisicion, la seleccion de proveedores, el ajuste de arreglos contractuales y la adquisicion en si. El hacerlo asi garantiza que la organizacion tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.
AI6	Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de produccion, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parametros del servicio) se deben registrar, evaluar y autorizar previo a la implantacion y revisar contra los resultados planeados despues de la implantacion. Esto garantiza la reduccion de riesgos que impactan negativamente la estabilidad o integridad del ambiente de produccion.
AI7	Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transicion e instrucciones de migracion, planear la liberacion y la transicion en si al ambiente de produccion, y revisar la post-implantacion. Esto garantiza que los sistemas operativos esten en linea con las expectativas convenidas y con los resultados.
DS1	Contar con una definicion documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicacion efectiva la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso tambien incluye el monitoreo y la notificacio oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineacion entre los servicios de TI y los requerimientos de negocio relacionados.
DS2	La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administracion de terceros. Este proceso se logra por medio de una clara definicion de roles, responsabilidades y expectativas en los acuerdos con los terceros, asi como con la revision y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva

Figura 12.4. Consulta Estándar
Fuente: Muñoz, A. (2014)

Anexo 13. Herramientas utilizadas en la Aplicación Web.

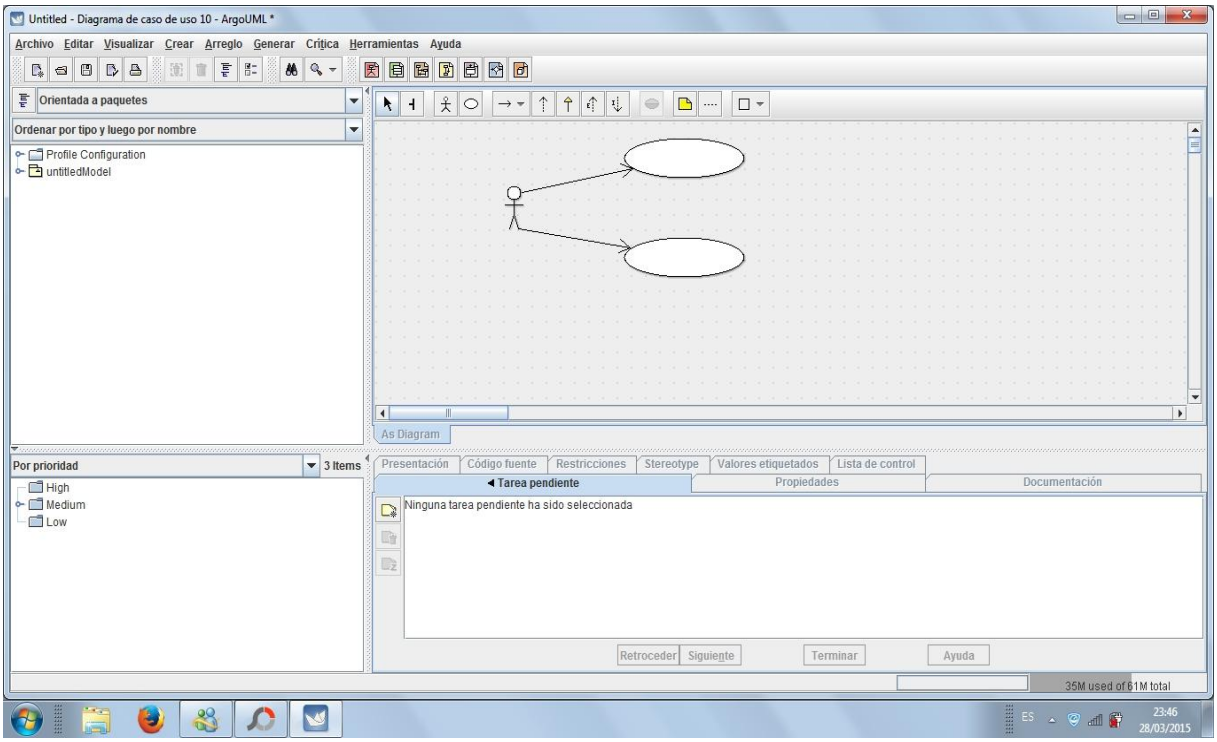


Figura: 13.1. Interfaz ArgoUml
Fuente. ArgoUml

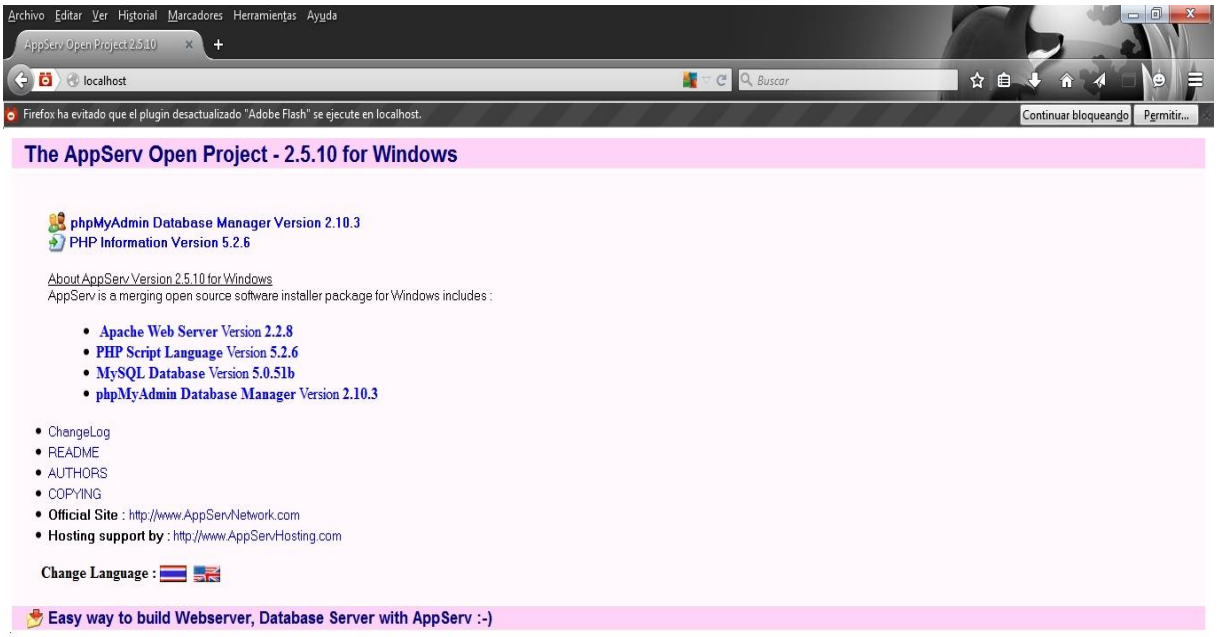


Figura: 13.2: Interfaz AppServ
Fuente: AppServ Open Project. 2.5.10

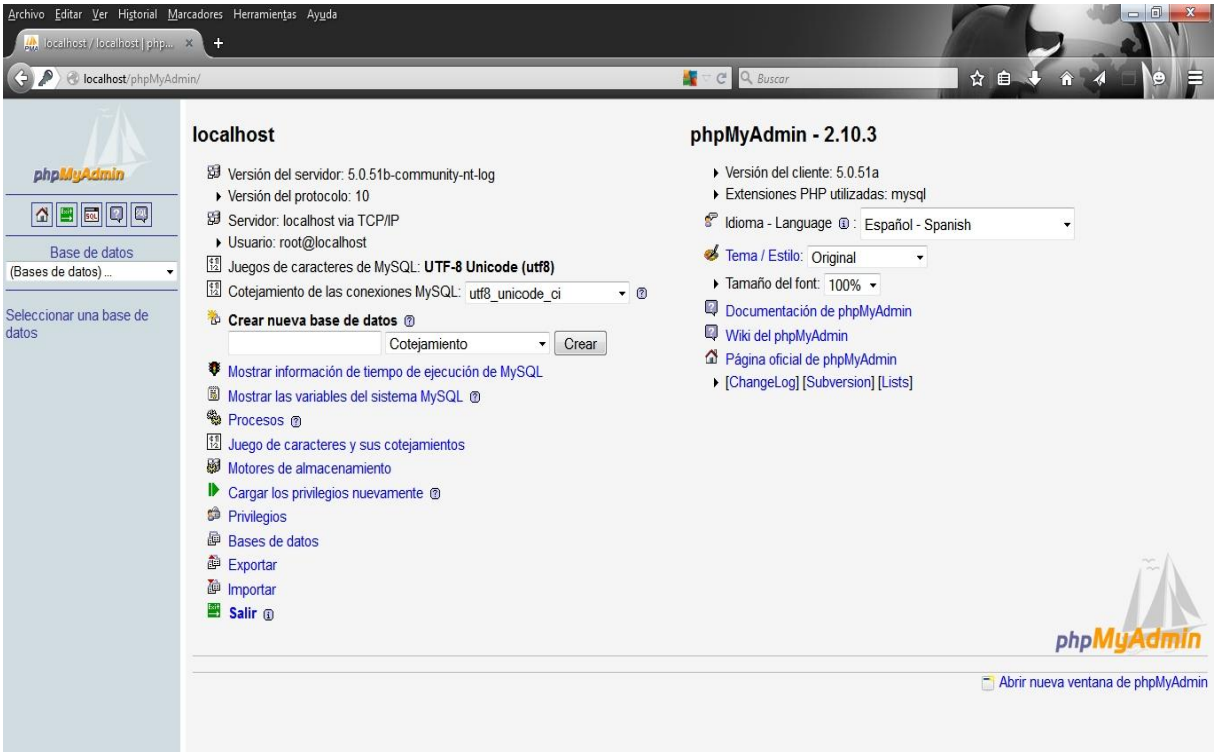


Figura: 13.3. Interfaz phpMyAdmin
Fuente: phpMyAdmin

Figura: 13.4. Intefaz Dreamweaver
Fuente: Macromedia Dreamweaver