UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

"Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT "

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

AUTORES:

BACH. YAN CARRANZA, FREDDY

BACH. ZAVALA VASQUEZ, CINTHIA LILIANA

ASESOR:

ING. DIAZ SÁNCHEZ, JAIME EDUARDO

TRUJILLO – PERÚ
2013

“*Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT*”

Elaborado por:

Bach. YAN CARRANZA, FREDDY

Bach. ZAVALA VASQUEZ, CINTHIA LILIANA

Aprobada por:

Ing. Karla Meléndez Revilla, CIP 120097
Presidente

Ing. Carlos Gaytán Toledo, CIP 84519
Secretario

Ing. Walter Moncada Carcamo, CIP 33829
Vocal

Ing. Jaime E. Díaz Sánchez, CIP 73304
Asesor

PRESENTACIÓN

Señores Miembros del Jurado:

De conformidad y en cumplimiento de los requisitos estipulados en el reglamento de grados y Títulos de la Universidad Privada Antenor Orrego y el Reglamento interno de la Escuela Profesional de Ingeniería de Computación y Sistemas, ponemos a vuestra disposición el presente Trabajo de Suficiencia Profesional titulado:“ Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT” para obtener el Título Profesional de Ingeniero de Computación y Sistemas mediante la modalidad de Tesis.

El contenido de la presente tesis ha sido desarrollado tomando como marco de referencia los lineamientos establecidos y los conocimientos adquiridos durante nuestra formación profesional, consulta de fuentes bibliográficas e información obtenida de la Gerencia Regional de Educación La Libertad.

Los Autores.

Bach. YAN CARRANZA, FREDDY

Bach. ZAVALA VASQUEZ, CINTHIA LILIANA
Ing. Estadístico. COESPE 494

DEDICATORIA

.

A Dios, por darme vida, me diste varias pruebas de fe, y a creer en los milagros.

A mis padres Susana y Hernán, por sus consejos y buenos deseos.

Al amor de mi vida Freddy, al cual amo cada día más.

A mis hermanos Carlos y Wendy, por su afecto y apoyo constante. A la vez a mí querida Zatomy quien descansa en paz en el cielo.

A mis amigos Oscar, Laly, Faby, Diego, Carmen y Christian, por ser mis compañeros de trabajo de los cursos, entre risas y renegadas se hicieron buenos proyectos.

DEDICATORIA

.

A Dios, por darme vida, me diste varias pruebas de fe, y a creer en los milagros.

A mis padres Genaro y Ana, papi taplenco me enseñaste en ser correcto, honesto y sobretodo puntual, mi mami por su incansable apoyo incondicional, por enseñarme principios, valores, y a nunca rendirme a pesar de todo, y siempre seguir adelante.

A mis hermanos, Genaro por molestarme a seguir mejorando y a no dejarme, mi hermana Magali por el apoyo económico para poder estudiar en la universidad, sus continuas quejas de mejorar los trabajos que presentaba, me ayudaron a mejorar en lo profesional, aun me sigues dando lecciones ("manzanitas").

A mi princesita bella Cinthia por su apoyo en los momentos difíciles, mi amiga, compañera de tesis y pareja gracias por seguir aguantándome.

A la memoria de mi linda wawita, gracias por ser mi despertador, por alegrarme los días.

A mi amigo Daniel por los días de relajo y tertulias de proyectos innovadores, seguimos en la lucha.

A mis amigos Víctor, Oscar, Laly, Diego, Ricardo, Jaime, Fiore, por ser mis compañeros de trabajo de los cursos, entre risas y renegadas se hicieron buenos proyectos.

AGRADECIMIENTO

A nuestro asesor el Ing. Jaime Díaz, quien por sus valiosos aportes tanto en lo profesional como en lo personal, nos ha permitido lograr la tesis. Gracias por todo

A los Ingenieros Karla Melendez, Carlos Gaytán y Walter Moncada, por su colaboración en la revisión y corrección del presente trabajo.

Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT

RESUMEN

Por: Freddy Yan Carranza
Cinthia Liliana Zavala Vásquez

La presente tesis tiene de capítulos, anexos, y tiene como principal objetivo Elaborar un Plan de Mejora de seguridad de la información y continuidad del Centro de Datos, y mostrar los resultados obtenidos de la auditoria de sistemas, utilizando la metodología MAIGTI, el marco de trabajo y las directrices de auditoría propuestas por lineamientos ISO 27001 y buenas prácticas COBIT 4.0.

El Capítulo I presenta una descripción de las definiciones, buenas prácticas, lineamientos y la Metodología utilizada, también del Marco Metodológico empleada en la tesis.

El Capítulo II detalla una visión de la situación actual del centro de datos de la GRELL y realización de la auditoria de sistemas, en donde se seleccionaran los procesos de control más adecuados propuestos por ISO 27001 y COBIT 4.0 que se ajusten a la situación actual del centro de datos, en donde se evaluará y se realizará recomendaciones. Al igual se presentará los resultados de la auditoria a través de un informe, en donde se mostrará el análisis de los resultados, y se entregará las conclusiones finales por cada proceso evaluado.

El Capítulo III detalla los planes de mejora, como la Implementación de un Sistema de Gestión de Seguridad de la Información redactando los objetivos, alcance, metodología, fases, entre otros y un Plan de Continuidad del Negocio con fases y un Plan de Normalización.

El Capítulo IV detalla la inversión de la solución.

Finalmente, se presentan las conclusiones y recomendaciones de la tesis.

Information Security and Data Center Continuity Improvement Plan for La Libertad Regional Office of Education applying ISO 27001 guidelines and COBIT best practices.

ABSTRACT

Por: Freddy Yan Carranza
Cinthia Liliana Zavala Vásquez

ABSTRACT

This thesis project consists of chapters, and appendices, which are aimed to develop a Plan to Improve information security and Data Center continuity, and show the results obtained from the information system audit, using the MAIGTI methodology, the ISO 27001 proposed framework and audit guidelines and COBIT 4.0 best practices.

Chapter I presents an overview of the definitions, best practices, guidelines and the methodology used, and also the methodological framework used in this thesis.

Chapter II describes an overview of the GRELL's data center current situation and the information system audit realization, where the most appropriate control processes that fit the data center current situation will be selected proposed by ISO 27001 and COBIT 4.0, where it will be evaluated and recommendations will be make. The audit results will also be presented through a report where the analysis results will be shown and the final conclusions for each evaluated process will be presented.

Chapter III details the improvement plans like the implementation of an Information Security Management System redacting the objectives, scope, methodology, phases, among others, a Business Continuity Plan with phases and a Normalization Plan.

Chapter IV details the solution investment.

Finally, this thesis project recommendations and conclusions are presented.

Tabla de Contenidos

PRESENTACIÓN 3

DEDICATORIA 4

DEDICATORIA 5

AGRADECIMIENTO 6

RESUMEN 7

ABSTRACT 8

ABSTRACT 8

INTRODUCCIÓN 12

Cap. I: FUNDAMENTO TEORICO 11

1.1 Conceptos/Definiciones 11
1.2 Métodos, Buenas Prácticas, Estándares 14
ITIL 14
COBIT 16
ISO/IEC 27001 21
ISO/IEC 17799 22
1.2.1 Normativas 24
1.3 Metodología 25
1.4 Marco Metodológico 28
1.4.1 Diseño de Contrastación 28
1.4.2 Tipo y Método de muestreo 29
1.4.3 Técnicas y Métodos de obtención de datos 29
1.4.4 Diseño de Instrumentos para la recolección de datos 30
1.4.5 Forma en que se analizarán e interpretarán los resultados de la investigación. 31
1.4.6 Estadísticas utilizadas para el análisis de la hipótesis de investigación. 31

Cap. II: RESULTADOS 32

2. Aplicación de la Auditoria de Sistemas 32

2.1 Prefacio 32
2.2 Diagnostico Preliminar 33
2.2.1 Descripción de la Empresa 33
2.2.2 Programa de Auditoria 34
2.2.3 Artefactos de Auditoría 36
2.3 Resultados de la Auditoria 52
2.3.1 RESUMEN EJECUTIVO 52
2.3.2 INTRODUCCIÓN 53
2.3.3 PROPUESTA TÉCNICA 54
2.3.4 Antecedentes 54
2.3.5 Objetivos 54
Etapa de Planificación 57
Etapa de Trabajo de Campo 57
Etapa de análisis y estructuración de la información. 57
Etapa de la Elaboración del Informe 58
2.3.6 EVALUACIÓN GENERAL 58

2.3.7 REVISIÓN DEL AVANCE DE IMPLEMENTACIÓN DE RECOMENDACIONES DE LA AUDITORIA ANTERIOR 69
2.3.8 CONCLUSIONES DE LA AUDITORIA 102

Capítulo III: PLAN DE MEJORA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD 104

3. SGSI Y PCN 104
3.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 104
3.1.1 OBJETIVOS 105
3.1.2 ALCANCE DEL DIAGNOSTICO SITUACIONAL INICIAL 105
3.1.3 METODOLOGÍA 105
3.1.4 DIAGNOSTICO SITUACIONAL INICIAL 106
3.1.5 TIEMPO DE IMPLEMENTACIÓN 107
3.1.6 CRONOGRAMA DE ACTIVIDADES 108
3.1.7 FASES Y ACTIVIDADES 109
3.1.8 CONSIDERACIONES A LA IMPLEMENTACIÓN DEL SGSI 115
3.1.9 DIFICULTADES DE UN SGSI 116
3.1.10 SELECCIÓN DE LA PLATAFORMA DE CONTROL Y LOS OBJETIVOS DE CONTROL 119
3.2 PLAN DE CONTINUIDAD DE NEGOCIO 120
3.2.1 Fases 122
3.2.2 Plan de Normalización de Servicios luego de la contingencia 123

Capítulo IV: REQUERIMIENTOS DE TI E INVERSIÓN DE LA SOLUCIÓN 127
4.1 COSTO DE LA INVERSIÓN 127

CONCLUSIONES 130

RECOMENDACIONES 132

REFERENCIAS BIBLIOGRÁFICAS 133

Tabla de Cuadros

Figura N° 1: Fundamentos de la Gestión de TI 15
Figura N° 2: Criterios y Recursos 19
Figura N° 3: Modelo Genérico de Madurez 21
Figura N° 4: Naturaleza de la forma ISO/IEC 27001:00 22
Figura N° 5: Cronograma del Proyecto 32

Tabla de Figuras

Cuadro N° 1: Lista de Objetivos de Control según ISO 1779 22
Cuadro N° 2: Cuadro Resumen Fases de Metodología 27
Cuadro N° 3: Cuadro Detalle Universo 28

INTRODUCCIÓN

En los últimos años todo lo relacionado respecto a seguridad de la información y continuidad de procesos suscita un gran interés. Las empresas y organismos del estado están más concientizados de los riesgos que conlleva la actividad electrónica.

En una época como la actual, donde estamos en un mundo globalizado, donde la información de los negocios ha tomado un papel muy relevante y en la que casi en su totalidad fluye por canales electrónicos, la continuidad del negocio depende de la seguridad y del flujo ininterrumpido de dicha información, esto explica el porqué es importante salvaguardar la información de la empresa en un lugar seguro y confiable.

En nuestra realidad, los problemas son muchos, la primera razón es que la gran mayoría de nuestros centros de datos han sido implementados sin ninguna normativa, al no tener las normativas no se va a contar con ninguna medida de seguridad, como procedimientos y controles en caso de alguna contingencia, entre otros.

Los centros de datos tienen que cumplir con ciertas características en cuanto la parte de la seguridad de la infraestructura física, y como se ve parte de la premisa de un buen diseño en cuanto es la confiabilidad, tenemos también ver la disponibilidad, seguridad al acceso del centro de datos con cualquier tecnología, también en seguridad a la ambientación, una buena climatización, refrigeración entre otros

La Gerencia Regional de Educación La Libertad no es ajena a esta problemática, es un órgano especializado del Gobierno Regional de La Libertad, encargados de asegurar la adecuación y aplicación de las políticas nacionales y regionales de educación, cultura, deporte, recreación, ciencia y tecnología y que aporta iniciativas propias para mejorar los niveles de aprendizaje de los niños, adolescentes, jóvenes y adultos, para mejorar la calidad educativa y como consecuencia el desarrollo integral de la población Liberteña.

La presente tesis busca diseñar un Plan de Mejora de la Seguridad de la Información y Continuidad para una institución del estado que cubra lo que pide la circular para evitar

problemas regulatorios con este organismo. Para esto, se utilizarán estándares y buenas prácticas reconocidas mundialmente para poder desarrollar una auditoria de sistemas y así poder tener una base que se pueda implementar un plan de mejora de seguridad y continuidad, aplicable a cualquier Centro de Datos. Cabe resaltar que estos estándares y buenas prácticas indican qué es lo que se debe realizar, pero no especifican cómo se deben implementar los controles. Estos van a depender de la necesidad de la empresa y de la inversión que desee realizar en temas de seguridad, con lo que se puede afirmar que por lo expuesto anteriormente y por los conocimientos que se tiene, en la presente tesis se propone la evaluación de una auditoría al Centro de Datos de la Gerencia Regional de Educación La Libertad, que permita mejorar la seguridad y la continuidad del Centro de Datos.

Por lo anterior, se formula el siguiente problema de investigación: "¿Cómo mejorar la seguridad de la información y continuidad de la operatividad del Centro de Datos de la Gerencia Regional de Educación La Libertad?" y su respectiva Hipótesis "Aplicando un Plan de Mejora basado en los lineamientos ISO/IEC 27001 y las buenas prácticas COBIT se mejorará la seguridad de la información y continuidad de la operatividad del Centro de Datos de la Gerencia Regional de Educación La Libertad."

Asimismo, el Objetivo General a conseguir es: "Elaborar un Plan de Mejora para el mejoramiento de seguridad de la información y continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad." Y sus Objetivos Específicos son:

a. Aplicar una Auditoría de Sistemas al Centro de Datos de la GRELL.
b. Identificar y evaluar los riesgos de TI asociados al Centro de Datos de la GRELL.
c. Identificar y evaluar los controles de TI existentes, asociados al Centro de Datos de la GRELL, basándose en COBIT, sobre la seguridad y continuidad de la información.
d. Identificar y Evaluar las normas de control interno para las TIC's implementadas en el Centro de Datos.
e. Evaluar los planes de contingencia y de continuidad de negocio asociados al Centro de Datos.

f. Elaborar el Plan de Mejora basándose en la NTP ISO/IEC 27001 y las Buenas Prácticas de COBIT 4.1.

Los aportes de la investigación son:

- Tecnológico: Uso eficiente de las tecnologías de información, para tener un mejor control en los ambientes computarizados para contribuir a la modernización y eficiencia, realizar evaluaciones de riesgos en ambientes de cómputo y diseñar los controles apropiados para disminuir esos riesgos.

- Sistémico: Uso seguro y adecuado de los sistemas de información bajo determinadas normas y buenas prácticas, para gestionar sus sistemas de forma rápida y segura, los Sistemas Informáticos están sometidos al control correspondiente.

El aporte que brinda este proyecto a la institución es de informar el estado actual de los sistemas de información y continuidad del Centro de Datos; así como las recomendaciones necesarias para superar las falencias encontradas según las buenas prácticas y alineamientos por COBIT e ISO/IEC 27001 respectivamente. También se proporcionará el Plan de Mejora para ser evaluado por la institución y así poder a implementar.

Cap. I: FUNDAMENTO TEORICO

1.1 Conceptos/Definiciones

Seguridad: Es el conjunto de medidas técnicas, educacionales, médicas y psicológicas empleadas para prevenir accidentes, eliminar las condiciones, inseguras del ambiente, e instruir o convencer a las personas, acerca de la necesidad de implantación de prácticas preventivas. (Contraloría General de la República)

Información: Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.(Real Académia Española)

Plan de Contingencias: es un documento de carácter confidencial que describe los procedimientos que debe seguir la Oficina e Informática para actuar en caso de una emergencia que interrumpa la operatividad del sistema de cómputo. (Contraloría General de la República)

Sistema de Información: está constituido por los métodos y procedimientos establecidos para registrar, procesar, resumir e informar sobre las operaciones de una entidad. La calidad de la información que brinda el sistema afecta la capacidad de la gerencia para adoptar decisiones adecuadas que permitan controlar las actividades de la entidad. (Contraloría General de la República)

Contraloría: La Contraloría General es el ente técnico rector del Sistema Nacional de Control, dotado de autonomía administrativa, funcional, económica y financiera, que tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental, orientando su accionar al fortalecimiento y transparencia de la gestión de las entidades, la promoción de valores y la responsabilidad de los funcionarios y servidores públicos, así como, contribuir con los Poderes del Estado en la toma de decisiones y con la ciudadanía para su adecuada participación en el control social. No puede ejercer atribuciones o funciones distintas a las establecidas

en la Constitución Política, en esta Ley, las disposiciones reglamentarias y las normas técnicas especializadas que emita en uso de sus atribuciones.(Contraloría General de la República)

Riesgo: La posibilidad de que ocurra un evento adverso que afecte el logro de los objetivos.(Real Académia Española)

Evento: Acaecimiento. Eventualidad, hecho imprevisto, o que puede acaecer. (Real Académia Española)

Impacto: El resultado o efecto de un evento. Puede existir una gama de posibles impactos asociados a un evento. El impacto de un evento puede ser positivo o negativo sobre los objetivos relacionados de la entidad. (Urbina Mancilla, 2006)

Integridad: está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio. (Institute, 2007)

Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas. (Institute, 2007)

Cumplimiento: tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas. (Institute, 2007)

Confiabilidad: se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.(Institute, 2007)

Centro de Datos: Cuando se habla del Centro de Datos se está refiriendo a la

ubicación donde concentran todos los recursos necesarios para el procesamiento de información de una organización.

Tecnologías de información y comunicación: Conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de información, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética.(Urbina Mancilla, 2006)

Concepto de las Normas de Control Interno: Las Normas de Control Interno, constituyen lineamientos, criterios, métodos y disposiciones para la aplicación y regulación del control interno en las principales áreas de la actividad administrativa u operativa de las entidades, incluidas las relativas a la gestión financiera, logística, de personal, de obras, de sistemas de información y de valores éticos, entre otras. Se dictan con el propósito de promover una administración adecuada de los recursos públicos en las entidades del Estado. Los titulares, funcionarios y servidores de cada entidad, según su competencia, son responsables de establecer, mantener, revisar y actualizar la estructura de control interno en función a la naturaleza de sus actividades y volumen de operaciones. Asimismo, es obligación de los titulares, la emisión de las normas específicas aplicables a su entidad, de acuerdo con su naturaleza, estructura, funciones y procesos en armonía con lo establecido en el presente documento. (Contraloría General de la República)

Auditoría: ISO (2002). A través de la norma ISO 19011:2002, indico las siguientes definiciones para los términos: Criterio de Auditoria, Evidencia de Auditoria, Auditoria y Hallazgos de Auditoria, las cuales se muestran a continuación:

Criterio de Auditoria es un conjunto de políticas, procedimientos o requisitos.

Evidencia de Auditoria comprende registros, declaraciones de hechos o cualquier otra información pertinente y verificable para los Criterios de Auditoría.

Auditoria es un proceso sistemático, independiente y documentado para obtener evidencia de la Auditoria y evaluarlas de manera objetiva con el fin de determinar

la extensión en que se cumplen los Criterios de Auditoría.

Hallazgos de Auditoría son los resultados de la evaluación de la Evidencia de Auditoría recopilada frente a los Criterios de Auditoría. Los Hallazgos de Auditoría pueden indicar conformidad o no conformidad con los Criterios de Auditoría u oportunidades de mejora.(Paredes, 2011)

1.2 Métodos, Buenas Prácticas, Estándares

ITIL

Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (**ITIL**) se ha convertido en el estándar mundial de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, **ITIL** es conocido y utilizado mundialmente. Pertenece a la OGC, pero es de libre utilización.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del coste, y el resto se invierte en el desarrollo del producto (u obtención). De esta manera, los procesos eficaces y eficientes de la

Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de coste aceptable.(ITIL-Gestión de Servicios TI) (Ver fig. 1).

ITIL es el enfoque más ampliamente aceptado para la gestión de servicios de TI en el mundo. ITIL proporciona un conjunto coherente de mejores prácticas, procedentes de los sectores público y privado a nivel internacional.(ITIL-Gestión de Servicios TI)

Figura N° 1: Fundamentos de la Gestión de TI

Fuente: ITIL- Gestión de Servicios TI- Consultora Osiatis

COBIT

a) Definición:

COBIT (Control Objectives for Information and related Technology).

Es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.(Institute, 2007)

Para ayudar a las organizaciones a satisfacer con éxito los desafíos de los negocios actualmente, el IT Governance Institute (ITGI) ha publicado la versión de COBIT 4.2

- COBIT es un framework de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de T.I. que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.
- COBIT hace posible el desarrollo de una política clara y las buenas prácticas para los controles de T.I. a través de las organizaciones.
- COBIT enfatiza en la conformidad a regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de la estructura COBIT.(Institute, 2007)

b) Estructura:

COBIT tiene 34 procesos genéricos agrupados en 4dominios, que cubren 215 objetivos de control, clasificados en cuatro dominios:

ISACA (1998) indicó que el COBIT comprende los siguientes grupos de objetivos de control:

- **Planificación y organización (PO):** Estrategias y tácticas. Identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio.
    a. Plan de informática alineado al Plan Estratégico de la organización

b. Planes de proyectos.
c. Plan de seguridad
d. Plan de continuidad de Negocio
e. Plan de Capacitación
f. Plan de Licenciamiento de Software
g. Plan de mantenimiento preventivo y correctivo
h. Plan de Calidad
i. Presupuestos
j. Estructura Organizacional
k. Recursos Disponibles
l. Metodologías de trabajo

- **Adquisición e Implementación (AI):** Identificación de soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes.
    a. Adquisiciones de tecnologías de la Información y afines: equipos de cómputo, equipos de red, licencias de software, sistema de información, etc.
    b. Propuestas técnicas
    c. Propuestas económicas
    d. Evaluaciones de proveedores
    e. Contratos
    f. Desarrollo de tecnologías de la información de base
    g. Desarrollo de sistemas de información
    h. Cumplimiento de metodologías y documentación respectiva.

- **Entregar y Dar Soporte (DS):** Cubre la entrega de los servicios requeridos. 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 operacionales.
    a. Entrega de servicios de Desarrollo e Implantación de Sistemas de Información

b. Evaluación de posibles soluciones de lo desarrollado o comprado e implantado
c. Medidas de Seguridad
d. Nivel de satisfacción de los usuarios con respecto al servicio otorgado
e. Entrega de servicios de Soporte Técnico
f. Infraestructura de Tecnologías de la Información: Hardware y Software de Base, así como servicios relacionados.

- **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.
    a. Seguimiento de los planes
    b. Evaluación interna del desempeño
    c. Certificaciones o acreditaciones independientes de control y seguridad
    d. Provisión de auditoría independiente(Paredes, 2011)

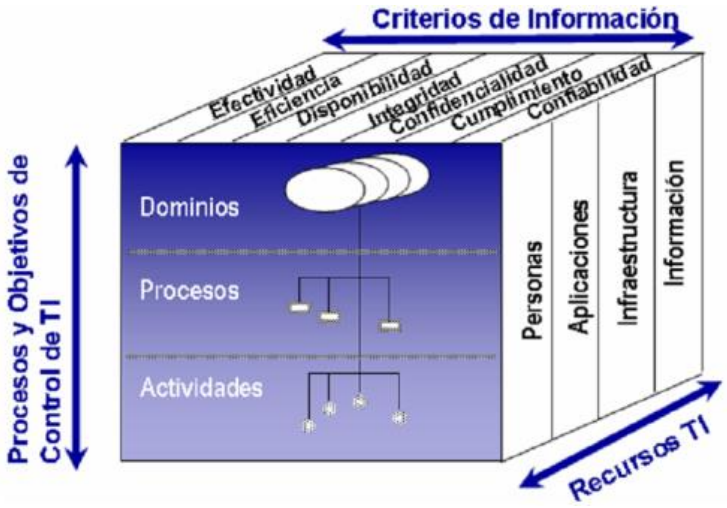
c) Criterios de Información y recursos de TI según COBIT:

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

- ✓ Efectividad: Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- ✓ Eficiencia: Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- ✓ Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada.

- ✓ Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- ✓ Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- ✓ Cumplimiento: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- ✓ Confiabilidad de la información: Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Figura N° 2: Criterios y Recursos



Fuente: IT Governance Institute

Los recursos de TI identificados en COBIT pueden identificarse/definirse como se muestra a continuación:

- ✓ Datos: Los elementos de datos en su más amplio sentido (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
- ✓ Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

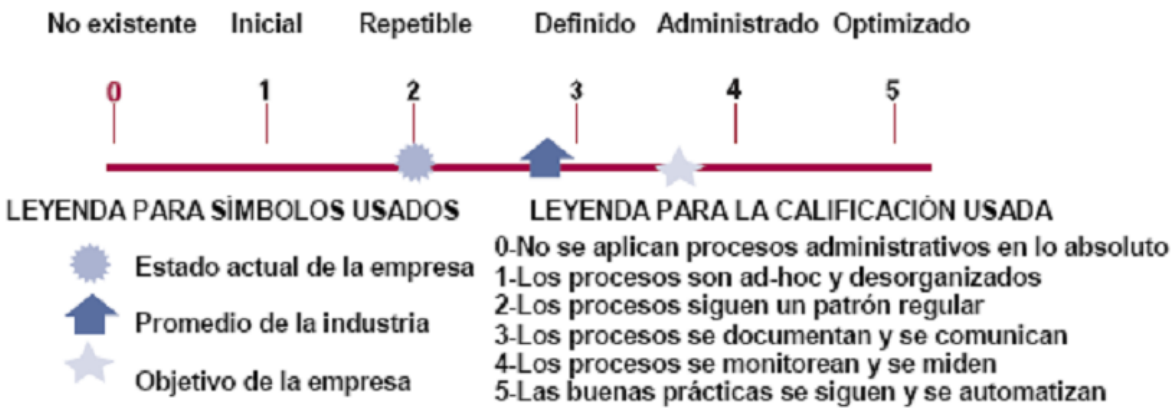
- ✓ Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.
- ✓ Instalaciones: Recursos para alojar y dar soporte a los sistemas de información.
- ✓ Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, soportar y monitorear servicios y sistemas de información.

d) Modelo genérico de madurez

- ✓ 0 – No Existente: 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 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, brindado herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Figura N° 3: Modelo Genérico de Madurez

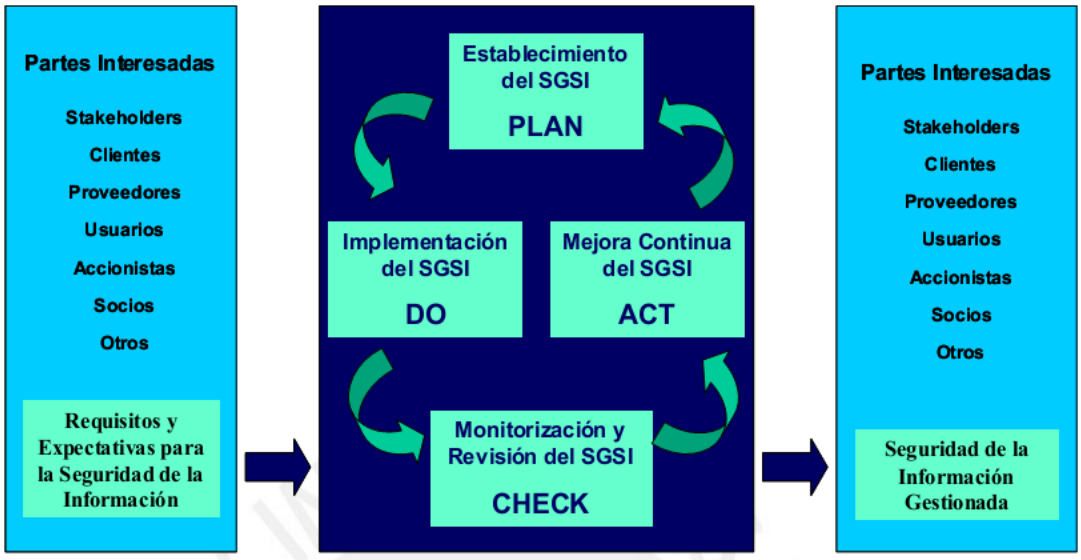


Fuente: IT Governance Institute

ISO/IEC 27001

Alexander (2007) indicó que el ISO/IEC 27001:2005 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un Sistema de Gestión de Seguridad de la Información para cualquier clase de organización. El diseño y la implantación se encuentran influenciado por las necesidades, los objetivos, los requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de organización. Está basado en el ciclo de Deming (Plan, Do, Check, Act) como se muestra en la siguiente figura:

Figura N° 4: Naturaleza de la forma ISO/IEC 27001:00



Fuente:(Paredes, 2011)

ISO/IEC 17799

ISO/IEC 17799 Código de Buenas Prácticas de Gestión de Seguridad de la Información, en la práctica, es una norma que provee una serie de objetivos de control para la gestión de procesos y proyectos de infraestructura de tecnologías de información. También incluye secciones relacionadas a la seguridad en el desarrollo de sistemas de información y a la gestión de la continuidad del negocio, entre otras. ISO/IEC 17799 incluye los siguientes grupos de objetivos de control:

Cuadro N° 1: Lista de Objetivos de Control según ISO 1779

A. Evaluación y Tratamiento del Riesgo	
B. Política de Seguridad	a. Documento de Política de Seguridad de la Información.
	b. Revisión y Evaluación
C. Aspectos Organizativos de la Seguridad	a. Estructura para la Seguridad de la Información: Comité, Recursos, Responsabilidades, Asesoría de Expertos, Colaboración entre Organización y Evaluación Independiente.
	b. Seguridad en los accesos de terceras partes Outsourcing.
D. Clasificación y Control de Activos	a. Responsabilidades sobre los activos

	b. Clasificación de la Información
E. Seguridad en Recursos Humanos	a. Seguridad antes del empleo
	b. Seguridad durante el empleo
	c. Finalización o cambio del empleo
F. Seguridad Física y del Entorno	a. Área Seguras
	b. Seguridad de los equipos
	c. Controles Generales
G. Gestión de Comunicaciones y Operaciones	a. Procedimientos y Responsabilidades de Operación
	b. Gestión de Servicios externos
	c. Planificación y Aceptación del Sistema
	d. Protección contra software malicioso
	e. Gestión de respaldo y Recuperación
	f. Gestión de Seguridad en redes
	g. Uso y seguridad de los medios de información
	h. Intercambio de Información y Software
	i. Servicio de correo electrónico
	j. Monitoreo
H. Control de Accesos	a. Requisito de negocio para el control de accesos
	b. Gestión de Acceso a Usuarios
	c. Responsabilidad de los usuarios
	d. Control de Acceso a Red
	e. Control de Acceso al sistema operativo
	f. Control de acceso a las aplicaciones
	g. Seguimiento de acceso y uso del sistema
	i informática móvil y teletrabajo
I. Adquisición, desarrollo y Mantenimiento de Sistemas	a. Requisito de la seguridad en los sistemas
	b. Seguridad de las aplicación
	c. Controles criptográficos
	d. Seguridad de los archivos del sistema
	e. Seguridad en los procesos de desarrollo y soporte
	f. Gestión de la vulnerabilidad técnica
J. Gestión de los Incidentes de la Seguridad de la Información	
K. Gestión de la Continuidad del Negocio	a. planificación
	b. Prueba
	c. Mantenimiento y revaluación de los planes de continuidad
L. Cumplimiento	a. cumplimiento de los requisitos legales
	b. revisiones de la política d seguridad y la conformidad técnica
	c. Consideraciones sobre la auditoria de sistemas

Fuente:(Paredes, 2011)

1.2.1 Normativas

Normas de control interno para sistemas computarizados

Los sistemas computarizados permiten a los usuarios ingresar a los documentos y programas en forma directa, ya sea a través de un microcomputador, conocido como computadora personal Lap Top (micro-computador portátil), o mediante terminales que se le denominan micro-computadoras en línea. Los controles internos que requieren los ambientes que emplean microcomputadoras son diversas y por lo general están referidos a los accesos, contraseñas, desarrollo y mantenimiento del sistema; los mismos que contribuyen a brindar seguridad y confiabilidad al procesamiento de la información.

Conforme surgen nuevas tecnologías, los usuarios emplean sistemas de cómputo cada vez más complejos, lo que incrementa las aplicaciones que manejan y, a su vez, aumenta el riesgo y plantea la necesidad de implementar nuevos controles internos.

Las normas de control interno que se presentan en esta sección describen los controles que son necesarios para la implementación del área de informática y el plan de sistemas de información de la entidad, según su actividad y durante un período determinado, así como los controles de datos fuente, de operación y de salida que preserven el flujo de información además de su integridad. Asimismo, tales normas desarrollan los controles internos requeridos para el mantenimiento de equipos de cómputo y medidas de seguridad para el Software (programas de computación) y Hardware (equipamiento informático), así como los aspectos de implementación del Plan de Contingencias de la Entidad. (Urbina Mancilla, 2006)

Norma general para el componente de información y comunicación

Se entiende por el componente de información y comunicación, los métodos, procesos, canales, medios y acciones que, con enfoque sistémico y regular, aseguren el flujo de información en todas las direcciones con calidad y oportunidad. Esto permite cumplir con las responsabilidades individuales y grupales.

La información no solo se relaciona con los datos generados internamente, sino también con sucesos, actividades y condiciones externas que deben traducirse a la forma de datos o información para la toma de decisiones. Asimismo, debe existir una comunicación efectiva en sentido amplio a través de los procesos y niveles jerárquicos de la entidad.

La comunicación es inherente a los sistemas de información, siendo indispensable su adecuada transmisión al personal para que pueda cumplir con sus responsabilidades.(Urbina Mancilla, 2006)

1.3 Metodología

MAIGTI (Metodología para la Auditoría Integral de Gestión de las Tecnologías de la Información).

MAIGTI enlaza los diversos conceptos de buenas prácticas del gobierno corporativo de gestión de las tecnologías de la información(COBIT de ISACA) , la gestión de los procesos de ciclo de vida de desarrollo de software (ISO/IEC 12207), las buenas prácticas de la gestión de la seguridad de la información (ISO/IEC 17799), la gestión de los servicios de tecnologías de información(ISO/IEC 20000 o ITIL); así como la gestión de Proyectos del Project Management Institute (PMOBOK), sobre la base de una simplificación del proceso general de auditoría descrito en la norma ISO 19011:2002 y de una adaptación del esquema de procesos de la ISO 9001:2000(ISO,2000). Se usarán estas normas y buenas prácticas por las siguientes razones:

a. El COBIT da un marco para la evaluación basado en el ciclo de calidad de Deming (Plan, Do, Check, Act).
b. Los estándares ISO/IEC 12207, ISO/IEC 17799 e ISO/IEC 20000 se complementan entres si, de manera que no existe cruce entre ellos si no interrelaciones muy útiles.
c. Si bien el PMBOK no es un estándar propio de la tecnología de información, contiene una serie de aspectos muy importantes con respecto a la gestión de proyectos alineados a la estrategia organizacional, además de complementar algunos aspectos de las normas citadas previamente, y

hacer referencia a metodologías de gestión de proyectos en relación a tiempo y costos, entre otros aspectos, que son muy útiles para la gestión de proyectos de tecnologías de información.

La estructura de la MAIGTI comprende los siguientes elementos:

a) Objetivo (la finalidad de la auditoría).
b) Alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría).
c) Entradas (requerimientos de información).
d) Proceso de MAIGTI (evaluaciones a realizar).
e) Salidas (papeles de trabajo e informe de auditoría).

Asimismo, cada uno de los procedimientos para la evaluación de los principales objetivos de control dentro de los subprocesos de MAIGTI, comprende la siguiente estructura: (a) objetivo (la finalidad del procedimiento de auditoría), (b) alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría a realizarse a través del procedimiento), (c) entradas (requerimientos de información para ejecutar el procedimiento de auditoría), (d) proceso (detalle de los pasos a seguir en el procedimiento de auditoría), y (e) salidas (hallazgos evidenciados como resultado de la ejecución del proceso).

Fig. Nº 4: Estructura de la MAIGTI

Fuente: MAIGTI- Emigdio Alfaro Paredes.

A continuación se lista las fases dadas dentro de la MAIGTI.

1. Determinar el Objetivo
2. Especificar el Alcance y Elaborar el Plan de Trabajo.
3. Solicitar la Información.
4. Recibir la Información. Ordenarla e Ingresarla al proceso MAIGTI.
5. Ejecutar el proceso MAIGTI.
    a. Evaluar DOC' s, Planificación y Organización.
    b. Evaluar DOC' s, Adquisición e Implementación.
    c. Evaluar DOC' s , Entrega de Servicio y Soporte
    d. Evaluar DOC' s, Monitoreo Y Control
    e. Ejecutar Procedimientos
6. Comunicar, Discutir y Corregir Informe
7. Distribuir Informe Final

Cuadro N° 2: Cuadro Resumen Fases de Metodología

Ítem	Fases de la Metodología	Descripción	Herramienta	Entregable
1	Objetivo	Detalla la finalidad para la cual se ha desarrollado el procedimiento.	Open Office 2010-(Writer,Calc),OpenProj - Project Management	Documento de Objetivos de la Auditoria, Cronograma de Trabajo
2	Alcance	Detalla de lo que está incluido y lo que no está incluido como parte de la auditoría: a) Evaluación de la Planificación y Organización b) Evaluación de la Adquisición e Implementación c) Evaluación de la Entrega de Servicios y Soporte d) D. Evaluación del Monitoreo y Control	Open Office 2010-(Writer, Calc),OpenProj - Project Management	Documento de Plan de Trabajo de Auditoría
3	Entradas	Detalla los requerimientos de información necesarios para el desarrollo del procedimiento	Open Office 2010-(Writer),OpenProj - Project Management	CheckList de Documentos Evaluados durante la Auditoría

4	Proceso	Detalla las actividades a ser realizadas como parte del procedimiento	Open Office 2010-(Writer), OpenProj - Project Management	Documento del Informe Preliminar e Informe final.
5	Salidas	Detalla las observaciones que se podría encontrar como resultado de la ejecución de las actividades del procedimiento	Open Office 2010-(Writer),OpenProj - Project Management	Papeles de Trabajo, Informe Final de Auditoria

1.4 Marco Metodológico

1.4.1 Diseño de Contrastación

Se Utilizara un diseño no experimental y descriptivo, porque no se manipularán las variables y se tiene la necesidad de indagar la incidencia y los valores que se manifiestan una o más variables, tal como lo definen (Hernández, R; Hernández, C. y P. Batista, 1997). En pocas palabras, se describe el fenómeno "tal cual" sin introducir modificaciones.

Además, exhibe el conocimiento de la realidad tal como se presenta en una situación "de espacio y de tiempo" dado. Aquí se observa y se registra, o se pregunta y se registra.

1.4.1.1 Universo

El universo de la investigación Plan de Mejora de la Seguridad y Continuidad del Centro de Datos de la Gerencia Regional de Educación de La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT, está constituida por 4 personas en las siguientes categorías:(Lopez, 1970)

Cuadro N° 3: Cuadro Detalle Universo

Empleados	2
Investigadores	2
Población	4

1.4.1.2 Muestra

No se realizará muestra porque se tomará en cuenta a toda la población debido a la cantidad del personal que está involucrado en el estudio los cuales solamente son 4.

1.4.2 Tipo y Método de muestreo

1.4.2.1 Tipo de muestreo

Como el método del muestreo utilizado fue el no probabilístico, el tipo aplicado fue el de dirigido o directo. Ya que permite seleccionar a la población adecuada, que pueda generar la información suficiente y necesaria para este estudio.

1.4.2.2 Método de muestreo

El método de muestreo empleado fue el no probabilístico, debido a que la elección de los elementos no depende que todas tengan la misma probabilidad de ser elegidos, sino de cumplir con ciertas características específicas según el objeto de la investigación.

1.4.3 Técnicas y Métodos de obtención de datos

- Entrevista: Esta herramienta se utilizará con los miembros que estén involucrados en el sistema, debido a que la población es pequeña y eso permitirá realizar una investigación más completa y directa.

  El auditor comienza a continuación las relaciones personales con el auditado lo hace de tres formas:

  1. Mediante la petición de documentación concreta.
  2. Mediante “entrevistas” en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
  3. Por medio de entrevistas en las que el auditor sigue un método

preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo.

Es necesario elegir bien a qué personas se va a entrevistar, y dependiendo del tema se elegirá normalmente entre directivos, jefes de proyecto, analistas, programadores, usuarios, operadores entre otros.

- Observación: Una de las técnicas más populares, de mayor impacto y más utilizadas para examinar los diferentes aspectos que repercuten en el funcionamiento del área, es la aplicación de diversas técnicas y métodos de observación que permiten recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas.(Razo, 2002)

1.4.4 Diseño de Instrumentos para la recolección de datos

- Lista de verificación o Checklist.

  Se realizará con el objetivo de capturar información de control, procedimiento y medidas seguridad; para validar la función de intervención de estos y los niveles de responsabilidad.

  Se diseñará una lista de verificación para cada procedimiento de control establecidos a utilizar dentro de la investigación, los cuales permitirán alcanzar el objetivo general de la investigación.

  El auditor, habitualmente informático de profesión percibe con cierta facilidad el perfil técnico y los conocimientos del auditado precisamente a través de las preguntas que este le formula. Esta percepción configura el principio de autoridad

y prestigio que el auditor debe poseer. El auditor deberá aplicar la Checklist de modo que el auditado responda clara y escuetamente (concisamente).

Se deberá interrumpir lo menos posible a éste, y solamente en los casos en las respuestas sean parte sustancialmente de la pregunta. En algunas ocasiones, se hará necesario evitar aquel a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

1.4.5 Forma en que se analizarán e interpretarán los resultados de la investigación.

Se realizará una recopilación de datos por medio del instrumento que se diseñará el cual tendrá que ser tabulado en una escala porcentual; cada pregunta tabulada pasará por un proceso de análisis para sacar conclusiones de dicha información.

1.4.6 Estadísticas utilizadas para el análisis de la hipótesis de investigación.

El instrumento a utilizar ***no tiene método estadístico*** definido por lo que no se sugiere algún estadístico a utilizar en especial para el análisis de las hipótesis de la investigación.

Cap. II: RESULTADOS

2. Aplicación de la Auditoria de Sistemas

2.1 Prefacio

Durante el desarrollo de este capítulo se conocerá más a fondo a la Gerencia Regional de Educación La Libertad., su descripción, su infraestructura y cómo está organizada estructuralmente, determinar cómo esta detallada su área de cómputo.

Con estos conocimientos previos se establece el plan de Auditoría de Sistemas, el cual contempla el objetivo principal, el alcance de la Auditoría, personal que va realizar la Auditoría, qué personas estarán involucradas, la ejecución de la Auditoría que contempla la recopilación de información, establecer una evaluación y clasificación de riesgos para poder determinar cuáles son los procesos más críticos y determinar observaciones que ayudarán a la Gerencia Regional de Educación La Libertad a controlar de mejor manera todo lo relacionado con Tecnologías de Información.

Para la ejecución de la Auditoría de Sistemas aplicando ISO 27001 y COBIT 4.0 se realizó el siguiente cronograma.

Figura N° 5: Cronograma del Proyecto

%	Nombre de tarea	Duraci	Comienzo	Fin
100%	Cronograma de Actividades del Proyeto:"Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT "	91 días	21/01/13	27/05/13
100%	**Inicio**	0 días	21/01/13	21/01/13
100%	**Elaborar el Plan de Proyecto de tesis**	11 días	21/01/13	04/02/13
100%	**Aprobación del Plan**	0 días	12/02/13	12/02/13
100%	**Desarrollo de la Metodología**	**64 días**	**12/02/13**	**10/05/13**
100%	**Fase I:Objetivo**	**3 días**	**12/02/13**	**14/02/13**
100%	Elaborar Documento de Objetivos de la Auditoría	2 días	12/02/13	13/02/13
100%	Elaborar Cronograma de Trabajo	1 día	14/02/13	14/02/13
100%	**Fase II: Alcance**	**8 días**	**15/02/13**	**26/02/13**
100%	Elaborar Documento de Plan de Trabajo de Auditoría	8 días	15/02/13	26/02/13
100%	**Fase III:Entradas**	**8 días**	**27/02/13**	**08/03/13**
100%	Elaborar Chek List de Documentos Evaluados durante la Auditoría	8 días	27/02/13	08/03/13
100%	**Fase IV:Proceso**	**15 días**	**11/03/13**	**29/03/13**
100%	Elaborar Documento de Informe Preliminar	15 días	11/03/13	29/03/13
100%	**Fase V: Salidas**	**30 días**	**01/04/13**	**10/05/13**
100%	Elaborar Papeles de Trabajo	15 días	01/04/13	19/04/13
100%	Elaborar Informe Final de Auditoria	15 días	22/04/13	10/05/13
100%	**Elaborar Informe de Tesis**	11 días	13/05/13	27/05/13
100%	**Fin**	0 días	27/05/13	27/05/13

2.2 Diagnostico Preliminar

2.2.1 Descripción de la Empresa

El Centro de Cómputo de la Gerencia Regional de Educación La Libertad tiene como función principal Administrar la Red Informática Local (LAN) que incluye: Administración de Cuentas de Usuario, Administración de estaciones de Trabajo, Administración de cada punto de la red de datos de la Institución.

Esto significa que para poder desarrollar las labores encomendadas por la actual gestión cumplen con los siguientes encargos:

- Velar por la seguridad física y lógica del parque informático de la DRELL el cual incluye hardware y Software.
- Velar por el buen funcionamiento de los gabinetes de comunicaciones y servidores los cuales reciben mantenimiento preventivo 03 veces al año.
- Salvaguardar las bases de datos de Sistema Único de Planillas, Sistema de Trámite Documentario, Sistema Nexus, SILEG y el AESCA (Sistemas de Escalafón), se generan copias de seguridad periódicamente.
- Brindar soporte técnico en hardware y software a los más de 100 usuarios con los que cuenta la Institución, atendiendo a sus llamadas cada vez que se requiera.
- Brindar apoyo en la parte informática ante cualquier solicitud de nuestros compañeros de trabajo: apoyo a eventos, elaboración de reportes específicos para presupuesto y planillas, apoyo técnico en elaboración de la declaración del formulario 600 al PDT de la SUNAT.
- Administrar el uso de Internet e Intranet, el cual se encuentra restringido sólo para uso de consultas concernientes al trabajo diario en esta Dirección Regional.
- Brindar soporte en la Instalación del Sistema de Trámite Documentario, así como administrar las cuentas de usuario del mismo.

2.2.2 Programa de Auditoria

OBJETIVO GENERAL	OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	HECHO POR	REF. PAPEL/TRABAJO
Elaborar el Plan de Mejora de la seguridad y continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad.	Verificar el estado actual de las recomendaciones de las auditorias anteriores	ME2	Monitorear y Evaluar el Control Interno.	Revisar las observaciones y recomendaciones de informes de auditorías anteriores así como su seguimiento.	PR01	Procedimiento para el seguimiento de informes de Auditoría Interna.	FY/CZ	**PT01:** Recomendaciones de las Auditorias Anteriores.
	Evaluar la Planeación y Estrategias de los Recursos de información.	PO1	Definir el Plan estratégico de TI.	Evaluar si los planes, estrategias y presupuestos de los sistemas de información son consistentes con las metas estratégicas y comerciales de la empresa.	PR02	Procedimiento para la auditoria de la Planificación Estratégica de Tecnología de Información.	FY/CZ	**PT02:** Planeación Estratégica de Tecnologías de Información.
		PO10	Administrar Proyectos.	Evaluar si los proyectos de TI están acordes con las necesidades de la empresa	PR03	Procedimiento para la auditoria de los Planes de Proyecto de Desarrollo de Sistemas de Información.	FY/CZ	**PT03:** Planes de Proyecto de Desarrollo de Sistemas de Información.
	Evaluar el estado de las Operaciones de los Sistemas de Información	DS11	Administrar los datos	Evaluar los procedimientos de respaldo	PR11	Procedimiento de auditoría para el mantenimiento de la biblioteca de medios	FY/CZ	**PT11:** Mantenimiento de Biblioteca de Medios.
					PR12	Procedimiento para la auditoria al procedimiento de eliminación de medios	FY/CZ	**PT12:** Procedimiento de Eliminación de Medios.
	Evaluar el adecuado Mantenimiento e implantación de los sistemas de Aplicación y Base de Datos	AI4	Facilitar la operación y el uso	Evaluar los manuales, políticas, normas y procedimientos que garanticen la adecuada gestión de las operaciones.	PR04	Procedimiento para la auditoria de la documentación de los manuales de usuario de los sistemas de información.	FY/CZ	**PT04:** Documentación de los Manuales de los Sistemas de Información.
					PR05	Procedimiento para la auditoria de los manuales de procedimientos de desarrollo de sistemas de información.	FY/CZ	**PT05**: Manuales de Procedimientos de desarrollo de sistemas de Información.
					PR06	Procedimiento para la auditoria de los manuales de procedimiento de soporte técnico	FY/CZ	**PT06:** Manuales de Procedimientos de Soporte Técnico.

OBJETIVO GENERAL	OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	HECHO POR	REF. PAPEL/TRABAJO
Elaborar el Plan de Mejora de la seguridad y continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad	Evaluar el adecuado Mantenimiento e implantación de los sistemas de Aplicación y Base de Datos	DS1	Definir y administrar niveles de Servicio	Evaluar que los niveles de servicio en los ambientes de procesamiento cumplan o superen las expectativas de la empresa.	PR07	Procedimiento para la auditoria de la metodología para la atención de requerimientos de soporte técnico	FY/CZ	**PT07:** Metodología Requerimiento de Soporte Técnico-Sistemas de Información.
					PR08	Procedimiento para la auditoria de la metodología para la atención de requerimientos de desarrollo de sistemas de información.	FY/CZ	**PT08:** Metodología de Requerimientos de Desarrollo-sistemas de Información
		AI7	Instalar y acreditar soluciones y cambios	Evaluar si los nuevos sistemas de aplicación se implantan de manera apropiada y funciona de acuerdo a las intenciones de la empresa.	PR09	Procedimiento para la auditoria de la metodología de desarrollo de sistemas de información	FY/CZ	**PT09:** Metodología de Desarrollo de Sistemas de Información.
		AI6	Administrar cambios	Evaluar si todas las modificaciones necesarias a los sistemas de aplicación existentes son implantadas oportunamente.	PR10	Procedimiento para la revisión de los formularios de control de cambios en proyectos de Compra o Desarrollo de Sistemas de Información	FY/CZ	**PT10:** Formularios de Control de Cambios.
	Evaluar el estado de la Seguridad de la información	DS5	Garantizar la seguridad de los sistemas	Evaluar los manuales, políticas y procedimiento que garanticen la adecuada seguridad de la información. Estructura de Gobierno de Seguridad de la Información.	PR13	Procedimiento para la auditoria del Plan de Seguridad de la Información	FY/CZ	**PT13:** Plan de Seguridad de la Información.
				Evaluación del Control de Accesos a los sistemas	PR14	Procedimiento para la auditoria de la seguridad de acceso a los sistemas de información	FY/CZ	**PT14:** Seguridad de Acceso a los Sistemas de Información.
				Evaluación del Control de Accesos a los centros de computo	PR15	Procedimiento para la auditoria de la seguridad de acceso al centro de cómputo principal	FY/CZ	**PT15:** Seguridad de Acceso al Centro de Computo Principal.
					PR16	Procedimiento para la auditoria de la seguridad de acceso al centro de cómputo alterno	FY/CZ	**PT16:** Seguridad de Acceso al centro de Computo Alterno.
	Evaluar el estado de la Gestión de Continuidad de Negocio	DS4	Garantizar la continuidad del servicio	Evaluar el Plan de recuperación de desastres	PR17	Procedimiento para la auditoria del Plan de Contingencias de Informática (PCI)	FY/CZ	**PT17:** Plan de Contingencias de Informática

2.2.3 Artefactos de Auditoría

2.2.3.1 Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Verificar el estado actual de las recomendaciones de las auditorias anteriores	ME2	Monitorear y Evaluar el Control Interno	Revisar las observaciones y recomendaciones de informes de auditorías anteriores así como su seguimiento	P01	P042 Procedimiento para el seguimiento de informes de Auditoría Interna	Revisar información de la auditoria de TI anterior	FY/CZ	27-02-13	28-02-13	Ejecutado
						Revisar detalladamente los informes de la auditoria de TI anterior				
						En los informes de auditoría anterior verificar la inclusión de las observaciones de los informes de otras auditorias anteriores				
						Identificar las observaciones de informes de auditorías anteriores que a la fecha no hayan sido subsanadas				
						Realizar el seguimiento de las observaciones de informes anteriores que a la fecha no hayan sido subsanadas (Entrevistas, muestreos)				

Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Evaluar la Planeación y Estrategias de los Recursos de información.	PO1	Definir el Plan estratégico de TI	Evaluar si los planes, estrategias y presupuestos de los sistemas de información son consistentes con las metas estratégicas y comerciales de la empresa.	P02	P005 Procedimiento para la auditoria de la Planificación Estratégica de Tecnología de Información	Revisar información del Plan estratégico de la organización, Plan estratégico de TI	FY/CZ	01-03-13	02-03-13	Ejecutado
						Verificar la alineación de los proyectos incluidos en el PETI y el Plan estratégico de la Organización				
						Verificar la elaboración de presupuestos y cronogramas claros para cada uno de los proyectos				
						Verificar la existencia de indicadores de Gestión				
	PO10	Administrar Proyectos	Evaluar si los proyectos de TI están acordes con las necesidades de la empresa.	P03	P006 Procedimiento para la auditoria de los Planes de Proyecto de Desarrollo de Sistemas de Información	Revisar información del PETI y el Plan estratégico de la organización	FY/CZ	04-03-13	04-03-13	Ejecutado
						Verificar la alineación de los proyectos al PETI y al Plan estratégico de la Organización				
						Verificar la asignación de presupuestos, cronogramas y responsabilidades de ejecución de los proyectos				
				P04	P007 Procedimiento para la auditoria de los Planes de Proyecto de Compra de Sistemas de Información	Revisar información Actas de reunión, Cotizaciones, Evaluación de la propuesta, Contrato para la compra de Sistemas de Información	FY/CZ	05-03-13	05-03-13	Ejecutado
						Verificar la alineación del Proyecto al PETI y Plan estratégico de la Organización				
						Verificar la existencia de análisis de Generación de valor del proyecto				
						Verificar la existencia de presupuesto adecuado para el proyecto				

Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Evaluar el estado de las Operaciones de los Sistemas de Información	DS13	Administrar las operaciones	Evaluar los manuales, políticas, normas y procedimientos que garanticen la adecuada gestión de las operaciones.	P05	P035 Procedimiento para la auditoria de la documentación de los manuales de usuario de los sistemas de información	Revisar información del listado de todo los manuales de usuario, acceso a todos los manuales de usuario y procedimiento para otorgar accesos a los manuales de usuario	FY/CZ	06-03-13	06-03-13	Ejecutado
						Revisar los manuales de usuario de los sistemas críticos del negocio.				
						Verificar el acceso de los usuarios a los manuales de usuario de los sistemas de información				
				P06	P040 Procedimiento para la auditoria de los manuales de procedimientos de desarrollo de sistemas de información	Revisar información de las Metodologías de Desarrollo utilizadas y Manuales de procedimientos de desarrollo de sistemas de información	FY/CZ	07-03-13	07-03-13	Ejecutado
						Verificar el cumplimiento del procedimiento de acuerdo a la metodología de desarrollo				
				P07	P039 Procedimiento para la auditoria de los manuales de procedimiento de soporte técnico	Revisión de la información de las metodologías y Manuales de procedimientos de soporte técnico	FY/CZ	07-03-13	07-03-13	Ejecutado
						Verificar el cumplimiento de los procedimientos de acuerdo a la metodología de soporte técnico				
	DS1	Definir y administrar niveles de Servicio	Evaluar que los niveles de servicio en los ambientes de procesamiento cumplan o superen las expectativas de la gerencia.	P08	P032 Procedimiento para la auditoria de la metodología para la atención de requerimientos de soporte técnico	Revisar información de metodologías de atención de requerimientos de soporte técnico	FY/CZ	08-03-13	08-03-13	Ejecutado
						Verificar la inclusión de Niveles de Servicio, para la atención de requerimientos de soporte técnico				
				P09	P033 Procedimiento para la auditoria de la metodología para la atención de requerimientos de desarrollo de sistemas de información	Revisar información de Metodologías de atención de requerimientos de desarrollo o mantenimiento ya sea si lo realiza personal interno o proveedor	FY/CZ	08-03-13	08-03-13	Ejecutado
						Revisar detalladamente la metodología y el Procedimiento de atención de requerimientos de desarrollo de sistemas de información ya sea con personal interno o proveedor				

Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Evaluar el estado de las Operaciones de los Sistemas de Información	DS13	Administrar las operaciones	Evaluar los manuales, políticas, normas y procedimientos que garanticen la adecuada gestión de las operaciones.	P05	P035 Procedimiento para la auditoria de la documentación de los manuales de usuario de los sistemas de información	Revisar información del listado de todo los manuales de usuario, acceso a todos los manuales de usuario y procedimiento para otorgar accesos a los manuales de usuario	FY/CZ	11-03-13	11-03-13	Ejecutado
						Revisar los manuales de usuario de los sistemas críticos del negocio.				
						Verificar el acceso de los usuarios a los manuales de usuario de los sistemas de información				
						Verificar el cumplimiento del procedimiento de acuerdo a la metodología de desarrollo	FY/CZ	11-03-13	11-03-13	Ejecutado
				P07	P039 Procedimiento para la auditoria de los manuales de procedimiento de soporte técnico	Revisión de la información de las metodologías y Manuales de procedimientos de soporte técnico	FY/CZ	12-03-13	12-03-13	Ejecutado
						Verificar el cumplimiento de los procedimientos de acuerdo a la metodología de soporte técnico				
	DS1	Definir y administrar niveles de Servicio	Evaluar que los niveles de servicio en los ambientes de procesamiento cumplan o superen las expectativas de la gerencia.	P08	P032 Procedimiento para la auditoria de la metodología para la atención de requerimientos de soporte técnico	Revisar información de metodologías de atención de requerimientos de soporte técnico	FY/CZ	12-03-13	12-03-13	Ejecutado
						Verificar la inclusión de Niveles de Servicio, para la atención de requerimientos de soporte técnico				
				P09	P033 Procedimiento para la auditoria de la metodología para la atención de requerimientos de desarrollo de sistemas de información	Revisar información de Metodologías de atención de requerimientos de desarrollo o mantenimiento ya sea si lo realiza personal interno o proveedor	FY/CZ	13-03-13	13-03-13	Ejecutado
						Revisar detalladamente la metodología y el Procedimiento de atención de requerimientos de desarrollo de sistemas de información ya sea con personal interno o proveedor				

Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Evaluar el adecuado Mantenimiento e implantación de los sistemas de Aplicación y Base de Datos	AI2	Adquirir y mantener el software aplicativo	Evaluar si los nuevos sistemas de aplicación se adquieren o desarrollan de acuerdo a las intenciones de la Gerencia	P10	P028 Procedimiento para la auditoria de los contratos para la compra de software de base	Revisar información de procedimientos para la generación de contratos para la compra de software Base (SB), cotizaciones, evaluación de las cotizaciones, Contratos y adendas para las compras de SB	FY/CZ	14-03-13	14-03-13	Ejecutado
						Revisar las cotizaciones y evaluaciones para la compra de SB				
						Revisar los contratos para la compra de SB				
	AI7	Instalar y acreditar soluciones y cambios	Evaluar si los nuevos sistemas de aplicación se implantan de manera apropiada y funciona de acuerdo a las intenciones de la empresa.	P11	P031 Procedimiento para la auditoria de la metodología de desarrollo de sistemas de información	Revisar detalladamente la metodología de desarrollo de software comparándola con la ISO 12207	FY/CZ	14-03-13	14-03-13	Ejecutado
						Revisar la ejecución de la metodología de desarrollo de sistemas de información				
	AI6	Administrar cambios	Evaluar si todas las modificaciones necesarias a los sistemas de aplicación existentes son implantadas oportunamente	P12	P047 Procedimiento para la revisión de los formularios de control de cambios en proyectos de Compra o Desarrollo de Sistemas de Información	Revisar información de la metodología de atención de requerimientos de desarrollo (controles de cambios) o mantenimiento de sistemas ya sea cuando lo realiza personal interno o proveedor, formularios de control de cambios funcionales y técnicos	FY/CZ	15-03-13	15-03-13	Ejecutado
						Revisar detalladamente la metodología de atención de requerimientos de desarrollo o mantenimiento				
						Revisar detalladamente los formularios de control de cambios funcionales y cambios técnicos para la compra de o desarrollo de sistemas de información				
	DS11	Administrar los datos	Evaluar los procedimientos de respaldo	P13	Procedimiento de auditoría para el mantenimiento de la biblioteca de medios	Revisar información de procedimientos de mantenimiento de la biblioteca de medios y eliminación de los medios de almacenamiento	FY/CZ	16-03-13	16-03-13	Ejecutado
						Revisar detalladamente el Procedimiento del mantenimiento de la biblioteca de medios de almacenamiento de datos				
				P14	Procedimiento para la auditoria al procedimiento de eliminación de medios	Revisar detalladamente el Procedimiento de eliminación de los medios de comunicación, equipos y medios de almacenamiento de datos	FY/CZ	16-03-13	16-03-13	Ejecutado

Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Evaluar el estado de la Seguridad de la información	DS5	Garantizar la seguridad de los sistemas	Evaluar los manuales, políticas y procedimiento que garanticen la adecuada seguridad de la información. Estructura de Gobierno de Seguridad de la Información.	P15	P010 Procedimiento para la auditoria del Plan de Seguridad de la Información	Revisar información del Plan de Seguridad de información, actas de reunión donde se aprueba el plan, Diagrama de Gantt para la ejecución de actividades del Plan de Seguridad	FY/CZ	18-03-13	18-03-13	Ejecutado
						Verificar la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Seguridad de Información				
						Verificar la alineación del Plan de Seguridad de Información al PETI				
						Verificar la implementación de las actividades indicadas en el Plan de Seguridad de Información				
			Evaluación del Control de Accesos a los sistemas	P16	P037 Procedimiento para la auditoria de la seguridad de acceso a los sistemas de información	Revisar información de listado de accesos de todos los usuarios sobre los sistemas de información, procedimiento para otorgar accesos a los sistemas de información	FY/CZ	19-03-13	19-03-13	Ejecutado
						Revisar detalladamente el perfil de accesos de cada personal y seleccionar los de mayor riesgos para posteriormente evidenciar el uso adecuado				
						Revisar detalladamente el procedimiento para otorgar accesos al personal verificando la autorización del Jefe de área y la unidad de riesgos				
			Evaluación del Control de Accesos a los centros de computo	P17	P054 procedimiento para la auditoria de la seguridad de acceso al centro de cómputo principal	Revisar información de listado de personas que tienen acceso al centro de cómputo, capacitación al personal de seguridad (vigilancia), Procedimiento para brindar acceso al centro de datos a personas ajenas a la organización	FY/CZ	20-03-13	20-03-13	Ejecutado
						Revisar el acceso por la puerta principal del edificio donde se encuentra el centro de datos principal				
						Revisar el acceso al piso donde se encuentra el centro de datos principal				
						Revisar el acceso al centro de datos principal				
						Analizar la pérdida de valor que se podría originar en caso de ser violentada la seguridad de acceso al centro de datos principal				
				P18	P056 Procedimiento para la auditoria de la seguridad de acceso al centro de cómputo alterno	Revisar información de listado de personas que tienen acceso al centro de cómputo alterno, capacitación al personal de seguridad (vigilancia), Procedimiento para brindar acceso al centro de datos alterno a personas ajenas a la organización	FY/CZ	21-03-13	21-03-13	Ejecutado
						Revisar el acceso por la puerta principal del edificio donde se encuentra el centro de datos alterno				
						Revisar el acceso al piso donde se encuentra el centro de datos alterno				
						Revisar el acceso al centro de datos alterno				
						Analizar la pérdida de valor que se podría originar en caso de ser violentada la seguridad de acceso al centro de datos alterno				

Cronograma de Ejecución de Procedimientos de Auditoria

OBJETIVOS	CODIGO	OBJETIVO CONTROL COBIT	COMPONENTE	N° PROC	PROCEDIMIENTOS DE CONTROL	ACTIVIDADES DE CONTROL	Responsable	Fecha Inicio	Fecha Fin	Estado
Evaluar el estado de la Gestión de Continuidad de Negocio	DS4	Garantizar la continuidad del servicio	Evaluar el Plan de recuperación de desastres	P19	P008 Procedimiento para la auditoria del Plan de Contingencias de Informática (PCI)	Revisar información del Plan estratégico de la Organización, PETI, Plan de contingencia Informática, Diagrama de Gantt del PCI	FY/CZ	22-03-13	22-03-13	Ejecutado
						Verificar la asignación de presupuesto, cronograma y responsabilidades para la elaboración del PCI				
						Revisar detalladamente la funcionalidad y claridad del PCI				
						Revisar el procedimiento de pruebas del PCI				
						Verificar la asignación de presupuesto, cronograma y responsabilidades para la ejecución del PCI				

2.2.3.2 Lista de Documentos a Solicitar

1. Descripción de la institución
2. Actividades y Ubicación donde se desarrolla los servicio de informática.
3. Diagrama Organizacional de TI
4. Descripción de funciones del personal de TI
5. Descripción del Departamento de Gestión de TI
6. Datos para el Contacto del responsable del departamento de la Gestión de TI
7. Descripción del Departamento de Desarrollo de Software
8. Datos para el Contacto del responsable del departamento de Desarrollo de Software
9. Descripción del Departamento de Soporte técnico
10. Datos para el Contacto del responsable del departamento de Soporte Técnico
11. Descripción del Departamento de Administración de Base de datos
12. Datos para el Contacto del responsable del departamento de Administración de Base de Datos
13. Descripción del Departamento de Operaciones
14. Datos para el Contacto del responsable del departamento de Operaciones
15. Descripción del Departamento de Seguridad de Información
16. Datos para el Contacto del responsable de Seguridad de Información
17. 2. Inventarios
18. Inventario de Software utilizado por GRELL
19. Inventario de Equipos de Cómputo utilizado por GRELL
20. 3. Información para ejecución de procedimientos de Control
21. Informe de Auditoría de TI anterior
22. Evidencias (email, informes, Cartas, PrintScreen, Memorando, Oficios, etc.) de seguimiento a las observaciones de informes de auditorías anteriores
23. Plan estratégico de la organización
24. Plan estratégico de TI
25. Plan de cada Proyecto de TI donde se incluya presupuestos, cronogramas y responsabilidades de ejecución del mismo
26. Actas de reunión donde se evalúe la compra de sistemas de información

27. Cotizaciones de compra de sistemas de información
28. Actas de reunión o documento donde se evalúe las propuestas para la compra del sistema de información
29. Documento de presupuestos para cada proyecto de TI
30. Lista de todos los manuales de usuario
31. Procedimiento de acceso a todos los manuales de usuario
32. Procedimiento para otorgar accesos a los manuales de usuario
33. Manuales de usuario de los sistemas críticos del negocio
34. Documentos donde se describan las Metodologías de Desarrollo de software utilizadas
35. Procedimiento de Desarrollo de sistemas de información
36. Documento donde se describa las Metodologías de soporte técnico utilizadas
37. Procedimiento de soporte técnico
38. Metodologías de atención de requerimientos de soporte técnico
39. Procedimiento de requerimientos de soporte técnicos, deberá incluir los SLAs
40. Metodologías de atención de requerimientos de desarrollo de sistemas de información
41. Procedimiento de requerimientos de desarrollo de sistema de información
42. Procedimientos para la generación de contratos para la compra de software Base (SB)
43. Cotizaciones para la compra de Software Base
44. Información de evaluación de las cotizaciones de compra de Software Base
45. Contratos y adendas a los contratos para las compras de Software Base
46. Metodología de desarrollo de software
47. Metodología de atención de requerimientos de desarrollo o mantenimiento de software (control de cambios en los sistemas)
48. Formularios de control de cambios funcionales en los sistemas
49. Formularios de control de cambios técnicos en los sistemas
50. Procedimientos de mantenimiento de la biblioteca de medios
51. Procedimiento de eliminación de los medios de almacenamiento
52. Plan de Seguridad de información
53. Actas de reunión donde se aprueba el Plan de Seguridad de Información

54. Diagrama de Gantt para la ejecución de actividades del Plan de Seguridad
55. Información de cumplimiento de actividades indicadas en el Plan de Seguridad de Información
56. Listado de accesos de todos los usuarios sobre los sistemas de información (Matriz de perfiles de usuarios)
57. Procedimiento para otorgar accesos a los sistemas de información
58. Listado de personas que tienen acceso al centro de cómputo principal
59. Evidencia de capacitación sobre control de acceso a las áreas restringidas (Centro de datos principal) dirigidas al personal de seguridad (vigilancia)
60. Procedimiento para brindar acceso al centro de datos principal a personas ajenas a la organización
61. Listado de personas que tienen acceso al centro de cómputo alterno
62. Evidencia de capacitación sobre control de acceso a las áreas restringidas (Centro de datos alterno) dirigidas al personal de seguridad (vigilancia)
63. Procedimiento para brindar acceso al centro de datos alterno a personas ajenas a la organización
64. Plan de contingencia Informática
65. Diagrama de Gantt de la elaboración del Plan de Contingencia Informática incluyendo (costos, actividades, cronograma y responsabilidades).

2.2.3.3 Cuestionarios

Ubicación y Construcción del Centro de Cómputo

1. ¿El edificio donde se encuentra la computadora está situado a salvo de?

   ¿Inundación? ()

   ¿Terremoto? ()

   ¿Fuego? ()

   ¿Sabotaje? ()

2. ¿El centro de cómputo da al exterior?
   SI NO

3. Describa brevemente la construcción del centro de cómputo; de preferencia tomando en cuenta el material con que fue construido, así como el equipo (muebles, sillas, etc.) del centro.

_____

4. ¿Tiene el cuarto de máquinas una instalación de escaparate y, si es así, pueden ser rotos los vidrios con facilidad?

   SI NO

5. ¿Está el centro de cómputo en un lugar de alto tráfico de personas?

   SI NO

6. ¿Se tiene materiales o paredes inflamables dentro el centro de cómputo?

   SI NO

7. ¿Se tiene paredes que despiden polvo?

   SI NO

8. ¿Se tiene paredes que no están adecuadamente selladas?

   SI NO

9. ¿Se tiene grandes ventanales orientados a la entrada o salida del sol?

   SI NO

10. ¿Existe lugar suficiente para los equipos?

    SI NO

11. ¿Está sobre saturada la instalación?

    SI NO

12. ¿Se tiene lugar previsto? Este es el adecuado para

Almacenamiento de equipos magnéticos	SI	NO
Formatos y papel para impresoras	SI	NO
Mesas de trabajo y muebles	SI	NO
Área y mobiliario para mantenimiento	SI	NO
Equipo de telecomunicaciones	SI	NO
Consola del operador	SI	NO
Área de recepción	SI	NO
Microcomputadoras	SI	NO
Fuentes de poder	SI	NO
Bóveda de seguridad (anti incendio, bajo máxima protección)	SI	NO

13. ¿Se tiene piso elevado?

    SI NO

    En caso afirmativo

14. ¿Está limpia la cámara plena?

    SI NO

15. ¿Está fácil la limpieza?

    SI NO

16. ¿El piso es antiestático?

SI NO

17. ¿La temperatura en la que trabajan los equipos es la recomendada por el proveedor?

SI NO

18. ¿Los ductos del aire acondicionado cuentan con alarmas contra intrusos?

SI NO

19. ¿Los ductos de aire acondicionado están limpios?

SI NO

20. ¿Se controla la humedad de acuerdo con las especificaciones del proveedor?

SI NO

21. ¿De qué forma?

_____

22. ¿Con que periodicidad?

_____

23. ¿Se cuenta con alarmas contra inundaciones?

SI NO

24. ¿Se han adoptado medidas de seguridad en el área de cómputo?

SI NO

25. ¿Existe personal responsable de la seguridad?

SI NO

26. ¿Existe personal de vigilancia en la institución?

SI NO

27. ¿Se investiga a los vigilantes cuando son contratados directamente?

SI NO

28. ¿Se controla el trabajo fuera del horario?

SI NO

29. ¿Se registra las acciones de los operadores para evitar que realicen alguna que pueda dañar el sistema?

SI NO

30. ¿Se identifica a la persona que ingresa?

SI NO

31. ¿De qué forma?

---

32. ¿Cómo se contra el acceso?

Vigilante	**( )**
Recepcionista	**( )**
Tarjeta de control de acceso	**( )**
Puerta de combinación	**( )**
Puerta con cerradura	**( )**
Puerta electrónica	**( )**
Puerta sensorial	**( )**
Registro de entradas	**( )**
Puertas dobles	**( )**
Escolta controlada	**( )**
Alarmas	**( )**
Tarjetas magnéticas	**( )**
Control biométricos	**( )**
Identificación personal	**( )**

33. ¿Existe vigilancia en el cuarto de máquina las 24 horas?

SI NO

34. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?

SI NO

35. ¿Son controladas las visitas y demostraciones en el centro de cómputo? ¿Cómo son controladas?

---

36. ¿Se registra el acceso al centro de datos de personas ajenas al área de cómputo?

SI NO

37. ¿Se tienen establecidos procedimientos de actualización para estas copias?

SI NO

38. Identifique el número de copias que se tienen, e acuerdo con la forma en que se clasifica la información

_____

39. ¿Existe departamento de auditoría interna en la institución?

SI NO

40. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?

SI NO

41. ¿Qué tipo de controles ha propuesto?

---

42. ¿Se cumplen?

SI NO

43. ¿Se auditan los sistemas en operación?

SI NO

44. ¿Con que frecuencia?

Cada seis meses **( )**

Cada año **( )**

Otra (especifique) **( )**

45. ¿Cuánto se efectúan modificaciones a los programas, a iniciativa de quién?

Usuario **( )**

Director **( )**

Jefe de cómputo **( )**

Otro(especifique) _____

46. ¿La solicitud de modificaciones a los programas se hacen en forma?

Oral **( )**

Escrita **( )**

(En caso de ser escrita solicite formatos) **( )**

47. Una vez adecuadas las modificaciones ¿Se presentan las pruebas a los interesados?

SI NO

48. ¿Existe control estricto en las modificaciones?

SI NO

49. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?

SI NO

50. ¿Se ha establecido el nivel de usuario de la información?

SI NO

51. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre el terminal y se dé aviso al responsable de ella?

SI NO

52. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?

SI NO

53. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones? ¿Cuáles son?

Recepción de documentos **( )**

Información confidencial	**( )**
Capacitación de documentos	**( )**
Cómputo electrónico	**( )**
Programas	**( )**
Discotecas y cintotecas	**( )**
Documentos de salida	**( )**
Activos magnéticos	**( )**

2.3 Resultados de la Auditoria

2.3.1 RESUMEN EJECUTIVO

El Data Center, se debe considerar aspectos sobre la Continuidad de Negocio, para lo cual se hace necesario adecuar y sincronizar los Planes de Continuidad del Negocio de La Gerencia Regional de Educación La Libertad, con los de El Ministerio de Educación, que deben estar enfocados a restablecer los Procesos Críticos del Negocio. Asimismo, se sugiere incluir dentro de las condiciones contractuales la programación de visitas periódicas al Data Center para verificar el cumplimiento de los controles de seguridad y de respaldo de información.

Como parte del proceso de cambio que viene experimentado la institución (reestructuración de la organización y el traslado del Data Center), se sugiere revisar y, de ser el caso, adecuar las Políticas y Procedimientos de Seguridad de Información de tal forma que se ajuste a esta nueva realidad.

Se está contemplando la instalación de un ambiente de pruebas, con lo cual se busca minimizar errores de los sistemas en el ambiente de producción. Para lograr una mayor efectividad en las pruebas se recomienda que este ambiente de prueba mantenga características idénticas al ambiente de producción (en lo que respecta al hardware, software y configuraciones). Asimismo, desde el punto de vista de confidencialidad de la información, se sugiere que los datos de pruebas sean distintos a los que se generan y procesan en el ambiente de producción.

Se percibe de las respuestas y entrevistas realizadas en el presente año, que, en líneas generales, los sistemas han mejorado y continúan en este proceso para satisfacer las necesidades internas y externas de los usuarios.

Es importante precisar que si bien no se cuenta con un Plan Estratégico de Tecnologías de Información (PETI), los servicios informáticos, se supervisan y controlan a través de reuniones permanentes en el área de Cómputo. Para revisar y evaluar los proyectos de tecnología.

De otro lado, se debe mencionar que las llamadas “Caídas” de los servidores, se han reducido con respecto al año 2012; sin embargo, se debe indicar que aún mantiene algunas dificultades.

2.3.2 INTRODUCCIÓN

El propósito principal de esta Revisión General de Sistemas es identificar recomendaciones y salvaguardas respectivas que se alineen a los objetivos de La Gerencia Regional de Educación La Libertad y que, a su vez, se ajuste a la normatividad vigente, sobre los servicios de auditoría de sistema de información que debe efectuar la institución.

El contenido del presente informe se basa principalmente en el (i) Levantamiento de Información, (ii) Análisis de Información, (iii) Validación de la Información y (iv) Emisión de Conclusiones y Recomendaciones con respecto a los puntos débiles o críticos detectados durante el estudio.

Durante la etapa de levantamiento de información se revisó y analizó el resultado de los cuestionarios resueltos por los Usuarios del Área de Cómputo, representado por la Jefa de Sistemas; (personal de las área de Cómputo). La información ha sido analizada de acuerdo a los siguientes frentes:

- Seguridad de Información
- Administración de las operaciones y comunicaciones
- Desarrollo y mantenimiento de sistemas de información
- Respaldo de Información
- Plan de Continuidad de Negocio
- Auditoría Interna
- Planificación
- Metodologías

La Auditoria de Sistemas se orienta a evaluar los sistemas de control dentro del ambiente de tecnología de información, con el fin de formular recomendaciones para mejorar estos mecanismos de control y/o proponer nuevos controles que se complementen a los actualmente implementados. La implementación de mejoras y nuevos controles tiene el propósito minimizar la ocurrencia de errores o riesgos futuros que pongan en peligro la gestión informática y, por lo tanto, genere un impacto desfavorable.

2.3.3 PROPUESTA TÉCNICA

2.3.4 Antecedentes

Un 22 de setiembre de 1962, se da el Decreto Ley 11209, con el cual se crean las Direcciones Regionales de Educación, cuyos fines fueron: Descongestionar el Ministerio de Educación Pública; la Diversificación del Sistema Educativo; Resolver la problemática Educativa en el mismo lugar donde se presentan; Descentralizar Administrativamente la Administración de la Educación Pública.

La Gerencia Regional de Educación, es el órgano de línea del Gobierno Regional La Libertad, encargado de asegurar la educación y aplicación de las políticas nacionales y regionales de educación, cultura, deporte, recreación, ciencia y tecnología, basado en valores con inclusión y equidad social, que aporta iniciativas para mejorar los niveles de aprendizaje de niñas y niños, adolescentes, jóvenes y adultos, para elevar la calidad educativa; contribuyendo al desarrollo integral de los Ciudadanos de la Región La Libertad

2.3.5 Objetivos

Objetivo General

Realizar un Estudio de Auditoría de Sistemas para La Gerencia Regional de Educación La Libertad, que permita evaluar la operación, uso de los sistemas de información, niveles de seguridad, procedimiento de respaldo, seguridad de los equipos de cómputo, redes y comunicaciones, evaluar el nivel de prestación de

servicios informáticos y de tecnología de información, con el fin de brindar las recomendaciones necesarias que se incorporen en forma integral a los sistemas de control y gestión de riesgos de tecnologías de información de la organización

Objetivos Específicos

- Evaluar los servicios informáticos que brinda soporte a las operaciones de la Institución.
- Identificar el nivel de riesgo existen sobre los distintos activos informáticos de La Gerencia Regional de Educación La Libertad, señalando las medidas correctivas que minimice la ocurrencia del riesgo.
- Evaluar los controles de respaldo de información y continuidad de negocio que actualmente mantiene la empresa.
- Determinar los niveles de seguridad física y lógica, así como el nivel de exposición al riesgo en La Gerencia Regional de Educación La Libertad, en aspectos de tecnologías de información.
- Determinar la calidad de los sistemas de información de La Gerencia Regional de Educación La Libertad en función a la operativa, tiempo de respuesta y uso de recursos informáticos (Hardware, Software, Redes y Comunicaciones).
- Identificar las recomendaciones necesarias referidas a la calidad del servicio prestado respecto a sistemas informáticos y a tecnología de información, de modo que respondan a los requerimientos internos de La Gerencia Regional de Educación La Libertad.

Alcance

- Realizar un diagnóstico y sus respectivas recomendaciones acerca de los procesos y uso de recursos en el Área de Sistemas, a fin de medir el grado de eficiencia, efectividad y rendimiento de los sistemas de La Gerencia Regional

de Educación La Libertad, acorde con los estándares ISO 27001 y de mejores prácticas COBIT.

- Efectuar una revisión general de la calidad de los sistemas de información de la Institución en función a los siguientes aspectos:
  - Disposición de todas las facilidades utilitarias de reorganización de archivos y copias de respaldo.
  - Disposición de procedimientos de respaldo ante caídas del sistema.
  - Óptima operativa del sistema de información.
  - Razonabilidad del consumo de los recursos informáticos y su nivel de planificación.
  - Mecanismos de seguridad, acceso y control de las operaciones.

- Realizar una revisión General de las características del esquema, funcionalidad, soporte y servicios de los sistemas de información actuales de la Institución y el uso de herramientas de tecnología de información:

  - Efectuar una evaluación general de la metodología de desarrollo de sistemas y de gestión de proyecto para los nuevos sistemas y la debida aplicación de los controles.
  - Efectuar una evaluación general de los planes existentes en la Organización (Plan Estratégico, Plan de Sistemas, Plan de Seguridad, Plan de Continuidad de Negocio, Plan de Capacitación, Plan de Adquisiciones), y su nivel de alineamiento a los objetivos estratégicos de la Institución.
  - Realizar una evaluación del avance de las implementaciones de las recomendaciones de la última **Auditoria de Sistemas** realizada.

2.3.5.1 Programa de Trabajo

El enfoque se ha empleado en la presente Auditoría de Sistemas se basa en la ejecución del siguiente programa:

Etapa de Planificación

- Elaborar cuestionarios dirigido a usuarios y al encargado del Área de Sistemas de acuerdo a los objetivos y alcance de la Auditoría de Sistemas.
- Coordinar la distribución de cuestionarios dirigidos al personal del Área de Cómputo.
- Recibir documentación solicitada de acuerdo a los resultados analizados en los cuestionarios.
- Identificar temas críticos según información preliminar proporcionada por la Institución.
- Preparar documentación para entrevistas al Área de Cómputo y áreas usuarias.

Etapa de Trabajo de Campo

- Revisar y analizar documentación entregada.
- Revisar y analizar cuestionarios recibidos.
- Efectuar entrevista al área de Cómputo con relación a los temas críticos de acuerdo al objetivo y alcance de la Auditoria de Sistemas.
- Efectuar entrevistas a las áreas usuarias con relación a lo temas críticos de acuerdo al objetivo y alcance de la Auditoria de Sistemas y de acuerdo al resultado de la entrevista con el área de Cómputo.
- Visitas al ambiente de cómputo y ubicación de equipos de comunicaciones.
- Revisión y evaluación de los Sistemas Informáticos.

Etapa de análisis y estructuración de la información.

Luego de analizar y revisar la información se procederá a ordenar las debilidades identificadas en la auditoria de sistemas y desarrollar las sugerencias de mejoras.

Etapa de la Elaboración del Informe

El informe de auditoría de sistemas se desarrollará a partir del análisis de resultado de cuestionarios, revisión de informes, entrevista con el responsable área de Cómputo, entrevistas con las áreas usuarias, inspección del ambiente de cómputo y comunicaciones, análisis de información y la identificación de sugerencias y recomendaciones.

2.3.5.2 Técnicas Utilizadas

En la evaluación efectuada se han empleado los siguientes procedimientos y técnicas generales:

- La Jefa de Cómputo, determinó quienes serían entrevistados (usuarios claves) para identificar el contexto del negocio (operaciones y servicios) y cómo éste es soportado por los sistemas de información; estas entrevistas permitieron también identificar la percepción de los usuarios entrevistados en relación al servicio que brinda el Área de Cómputo y la calidad de los sistemas informáticos.

- Cruce de Información. Mediante cruce de información documental, las entrevistas y cuestionarios se pudo confirmar hechos que evidenciaban una determinada debilidad.

2.3.6 EVALUACIÓN GENERAL

2.3.6.1 Aspectos del Plan de Seguridad de Información

En esta etapa se realizó la verificación del Plan de Seguridad de la información – PSI, el cual debe hacer referencia a los activos tecnológicos que deben ser protegidos de posibles riesgos, así como las estrategias de mitigar dichos riesgos. La verificación del PSI busca determinar el grado de desarrollo en cuanto a la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que la

información cumpla los criterios de confidencialidad, integridad y disponibilidad; en tal sentido se ha evaluado el PSI en función de:

- Definición de una política de seguridad.
- Evaluación de riesgos de seguridad a los que está expuesta los activos de información.
- Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.
- Plan de implementación de los controles y procedimientos de revisión periódicos.
- Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la institución, así como mantener pistas adecuadas de auditoría.

Para la verificación y evaluación del PSI se tomó como referencia dos documentos entregados por el Área de Cómputo: (i) Manual de Seguridad de Información y (ii) Políticas y Procedimientos. Asimismo, se sostuvo una reunión con personal del área de cómputo fin de discutir sobre los aspectos mencionados.

2.3.6.2 Aspectos de la Seguridad de Información

En esta etapa se realizó la verificación de los niveles de seguridad:

- Seguridad Lógica: Existencia de políticas para el control de acceso a los sistemas de información, redes y sistemas operativos
- Seguridad del personal: Existencia de procedimientos que permitan reducir los riesgos asociados al error humano, robo, fraude o mal uso de activos entre otros vinculados al riesgo de tecnología de información.

- Seguridad física y ambiental: Existencia de controles físicos al acceso, daño o interceptación de información, esto incluirá la revisión de instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

- Clasificación de la seguridad: Existencia de inventarios periódicos de activos asociados a la tecnología de información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de dichos activos

  Para la verificación y evaluación de los aspectos de la Seguridad de Información se tomó como referencia los documentados entregados por el Área de Cómputo: Roles y Responsabilidades del Personal y Manual de Seguridad de Información. Asimismo, se sostuvieron entrevistas y encuestas con personal usuario clave y una reunión con personal de sistemas a fin de discutir sobre los aspectos mencionados.

  En la presente auditoria no se ha identificado ninguna observación relevante referida a este aspecto. Sin embargo, se debe precisar que más adelante se abordará temas relacionados a este aspecto de la pasada Auditoría realizada.

2.3.6.3 Aspectos de la Administración de Operaciones y Comunicaciones

En esta etapa se realizó la verificación de las medidas de administración de las operaciones y comunicaciones que entre otros aspectos contiene lo siguiente:

- Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos

- Control sobre los cambios del ambiente de desarrollo al de producción.

- Separación de funciones para reducir el riesgo de error o fraude.

- Separación del ambiente de producción y el de desarrollo.

- Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.

- Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.

- Seguridad sobre correo electrónico.

Para la verificación y evaluación de la Administración de Operaciones y Comunicaciones se tomó como referencia los documentos entregados por el Área de Cómputo: Roles y Responsabilidades del Personal y Políticas y Procedimientos. Asimismo, se realizaron pruebas con algunos módulos del sistema con el propósito de realizar una evaluación general sobre el nivel de respuesta del mismo, se sostuvieron entrevistas y encuestas con personal usuario clave, reunión con personal de sistemas a fin de discutir sobre los aspectos mencionados.

De acuerdo a la información proporcionada, los cambios realizados en las instalaciones del Data Center, impactó sobre servicio informático durante dos días en el cual se tuvieron que realizar las actividades de manera manual. Esto no fue significativo en las operaciones de la institución.

2.3.6.4 Aspectos del Desarrollo y Mantenimiento de Sistemas de Información

En esta etapa se realizó la verificación de las medidas de desarrollo y mantenimiento de sistemas de información que entre otros aspectos contiene lo siguiente:

- Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles el ingreso, el procesamiento y la información de salida.

- Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.

- Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.

- Controlar el acceso a las librerías de programas fuente.

- Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

SITUACIÓN ACTUAL	RIESGO ASOCIADO	RECOMENDACIONES
Actualmente no se cuenta con una ambiente de pruebas en el cual se pueda realizar las pruebas de esfuerzo (stress) e identificar problemas de performance de estos sistemas que ayuden a mejorar los tiempos de respuesta. Actualmente, esta prueba se viene desarrollando en el ambiente de desarrollo.	La réplica de la Base de Datos de Producción al ambiente de Pruebas permitirá, de alguna forma, mejorar la realización la efectividad de las pruebas (por ejemplo, pruebas de esfuerzo). Sin embargo, el acceso de esta Base de Datos con información de producción en el ambiente de pruebas, puede generar problemas de confidencialidad de información.	Se recomienda que el Ambiente de Pruebas sea de características idénticas al ambiente de producción (hardware, software y configuraciones), para garantizar que el proceso de pruebas sea más efectivo. Se recomienda aplicar mecanismos de transformación de datos para evitar que en ambiente de prueba se utilicen datos que se trabaja en producción y, de esa forma, proteger la confidencialidad de la información.
No se cuenta con un Sistema de Gestión de la Calidad, para asegurar la buena performance de los sistemas de información en Producción.	Existe la probabilidad que existan errores en los sistemas de información en el ambiente de producción debido a una limitada aplicación de controles de calidad.	Establecer y mantener un Sistema de Gestión de la Calidad que considere los siguientes aspectos: – Responsables de control calidad (evaluar si es necesario implementar un comité como parte de la organización de la gestión de

SITUACIÓN ACTUAL	RIESGO ASOCIADO	RECOMENDACIONES
		calidad). – Definición de criterios de calidad. – Definición de procesos claves de TI su secuencia e interacción con otros procesos. – Políticas, criterios y métodos para descubrir actividades erradas. – Procedimientos para supervisar y medir la eficacia y aceptación del QA y aplicar proceso de mejoramiento continuo La implantación de un Sistema de Control de Calidad tiene el propósito de minimizar los errores (o "caídas") de los sistemas de información, así como también poder detectar los problemas de performance antes que éstos ingresen a Producción.

2.3.6.5 Aspectos de los Procedimientos de Respaldo

En esta etapa se realizó la verificación de los procedimientos de respaldo regulares periódicamente validados. Estos deben incluir las medidas necesarias para asegurar la recuperación en caso de falla en los medios o luego de un evento mayor. Estas medidas deben ser coherentes con la estrategia de continuidad de negocios de la institución y deben evitar que la información de respaldo y los procedimientos de restauración estén expuestos ante posibles eventos que comprometan la operación del centro principal de procesamiento.

Para la verificación y evaluación del Desarrollo y Mantenimiento de Sistemas de Información se tomó como referencia el documento entregado por el Área de Cómputo: Políticas y Procedimientos.

2.3.6.6 Aspectos del Plan de Continuidad de Negocio

En este punto se verifica que la institución cuente con el "Plan de Continuidad de Negocios" (PCN), el cual debe ser periódicamente validado, garantizando de esta manera un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

SITUACIÓN ACTUAL	RIESGO ASOCIADO	RECOMENDACIONES
Los Servidores están ubicados en las Instalaciones del segundo piso de la Institución. De acuerdo a información proporcionada en las entrevistas, El ministerio de educación tiene un Plan de Continuidad de Negocio para su Data Center.	Existe la probabilidad que, por desconocimiento del personal y por falta de pruebas al plan, no se desarrollen todas las actividades de recuperación de operaciones de manera adecuada durante un evento de emergencia.	Se recomienda: – El Plan de Continuidad de Negocio de La Gerencia Regional de Educación La Libertad debe estar sincronizado con el Plan del Ministerio de Educación – Planificar y ejecutar pruebas del Plan de Continuidad de Negocio, donde se pruebe la sincronización y consistencia con el Plan de la GRELL.

2.3.6.7 Aspectos de la Auditoría Interna

En esta etapa se verificó que la institución cuente con un servicio permanente de auditoría de sistemas, que colaboré con el área de auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, dentro del marco del plan de auditoría anual

En la presente auditoria no se ha identificado ninguna observación relevante referida a este aspecto.

2.3.6.8 Aspectos Metodológicos

Según las mejores prácticas de Tecnologías de Información expuestas en COBIT en su procedimiento P010 la institución deben seguir procedimientos que aseguren una correcta Administración de Proyectos. En tal sentido, en esta etapa se verificó que la institución cuente con metodologías de gestión de proyectos y con formatos de documentación estándar.

Actualmente el desarrollo de Sistemas se realiza mediante una Metodología propia. En la presente auditoria no se identificó ninguna observación relevante con relación al aspecto de metodologías.

2.3.6.9 Aspectos de Planificación

En esta etapa se verificó que la institución cuente con planes operativos, planes estratégicos, entre otros, que le marquen el camino a seguir con respecto a las tecnologías de información dentro un periodo. Para este propósito se usó como referencia el procedimiento P01 Definir Plan Estratégico TI expuesto en la versión 4.1 de COBIT.

Para la verificación y evaluación de los Aspectos de Planificación se tomó como referencia la reunión sostenida con el Jefe de Desarrollo de Proyectos y posteriormente con el Jefe de Producción, que fue designado por el Gerente Regional de Educación La Libertad, en su reemplazo.

A la fecha aún no cuenta con un Plan Estratégico de Tecnología de Información que marque la tendencia tecnológica de mediano y largo plazo de acuerdo al Plan Estratégico de La Gerencia Regional de Educación La Libertad (estrategias de hardware, software, comunicaciones y personal). Ésta fue una observación de la Auditoría 2009. Más adelante, en el punto 3.5 “Estado al 2013”, se revisa el estado de esta observación.

2.3.7 REVISIÓN DEL AVANCE DE IMPLEMENTACIÓN DE RECOMENDACIONES DE LA AUDITORIA ANTERIOR

ASPECTOS DEL PLAN DE SEGURIDAD DE INFORMACION			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
De acuerdo al documento denominado Manual de Seguridad de Información elaborado por sistemas GRELL; el cual es de aplicación del personal de GRELL y del personal de las instituciones asociadas; se tiene por objetivo crear un conjunto de reglas básicas que rijan el comportamiento del personal en el uso de información para el desarrollo de sus tareas. Asimismo, en el documento 1.12 Políticas y Procedimientos se han definido, como parte del capítulo	Si bien se definen los proyectos de TI que deberán ser desarrollados como mínimo a lo largo del año y estos son identificados con las áreas de negocio; no se cuenta con un Plan Estratégico de Tecnología de Información formalmente desarrollado. En tal sentido existe el riesgo que los documentos en donde se amplía el Plan de Seguridad de Información no esté correctamente alineado con los objetivos estratégicos del negocio persigue; sea por falta de actualización o por falta de identificación formal de nuevos activos de tecnología de información que soportan las estrategias del negocio.	Formalizar el Plan Estratégico de Tecnologías de Información (PETI) y, en base a la orientación tecnológica del negocio, desarrollar el Plan de Seguridad de Información que se alinee a éste. Tal como establecen las buenas prácticas de Control Interno de Tecnologías de Información (*Ver Cobit 4.1 Procedimiento P01 Definir el Plan Estratégico de TI – Control Objectives for Information and related Technology*), el desarrollo del	Se está reestructurando la organización a fin de fortalecer el cumplimiento de todos los objetivos de la Institución, lo cual permitirá facilitar el desarrollo apropiado de los planes y Sistemas de Información. En este contexto se proyecta formalizar el Plan Estratégico de Tecnologías de Información (PETI) y otros planes, tal como el Plan de Seguridad de Información. Se estima que en el Primer Trimestre 2013, ya se cuente con algunos resultados.

ASPECTOS DEL PLAN DE SEGURIDAD DE INFORMACION			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
Administración de Seguridad de Información, Objetivos de Control y Acciones referidos a los siguientes factores: Exposiciones y Controles de Acceso Lógico, Seguridad de Infraestructura de Red, Exposiciones y Controles Ambientales, Exposiciones y Controles de Acceso Físico. Ambos documentos tienen una orientación de control y de salvaguarda de la información que GRELL administra; sin embargo, se observa que se puede reforzar la gestión de la seguridad de información si éste respondiera a un		PETI es importante, puesto que facilita la orientación de TI del negocio y permite establecer los estándares técnicos de mediano y largo plazo. <u>Beneficios</u>: 1. Actualización permanente de los controles de Seguridad de Información. 2. Aseguramiento en la razonabilidad al implementar controles de Seguridad de Información alineados al negocio específicos de GRELL	

ASPECTOS DEL PLAN DE SEGURIDAD DE INFORMACION			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
Plan Estratégico de TI orientado al negocio y de actualización periódica.		3. Involucramiento de las áreas de negocio en la Seguridad de Información desde la definición de los objetivos estratégicos de TI e identificación de activos de información. 4. Respuesta inmediata a requerimientos para revisar el cumplimiento de normatividad vigente.	

ASPECTOS DEL PLAN DE SEGURIDAD DE INFORMACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
El Manual de Seguridad de Información hace referencia a Activos de Información: Información, Equipos que la soportan y personas que la utilizan; sin embargo falta identificar de manera detallada los activos específicos que requieren ser protegidos según el grado de exposición al riesgo en el que se encuentran.		Realizar un inventario de activos asociados a la Tecnología de Información, realizar un análisis de los riesgos a los cuales cada uno de éstos se encuentra expuesto, asignar una clasificación de los mismos en función de la exposición de los riesgos, con lo cual se identifiquen objetivos de control para los Activos críticos. Beneficios: 1. Focalización de esfuerzos hacia la protección de activos críticos 2. Facilita la señalización,	El área de cómputo, está en proceso de completar el inventario de activos y debe culminar esta actividad antes que finalice el presente año. Se obtendrá, a través de este proceso, un inventario que permita la precisión en la gestión de cambios y facilita la gestión de riesgos

ASPECTOS DEL PLAN DE SEGURIDAD DE INFORMACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		tratamiento y protección de los activos de información. 3. Facilita el análisis de causas ante incidentes que afecten la confidencialidad, integridad y disponibilidad de los recursos TI.	

ASAPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
El procedimiento de Control de Ingreso al Centro de Cómputo no existe. Es por ello que en la actualidad en GRELL, no se cuenta con un Sistema de Acceso al Centro de Cómputo.	Se hace necesario la Revisión permanente y la Actualización del procedimiento de acceso para garantizar la Seguridad del Equipamiento y el Control de acceso periódico para verificar el cumplimiento de los mismos.	Revisar y actualizar el procedimiento de Control de Ingreso al Centro de Cómputo y realizar un seguimiento periódico que facilite la actualización del procedimiento en función del historial de eventos que se hayan producido entre el periodo comprendido entre una revisión y otra. Beneficios: 1. Alineamiento de las actividades de control en función a hechos o eventos concretos. Actualización en	Se recomienda revisar el nuevo servicio ofrecido por MINISTERIO del Perú, en el Data Center, que debe considerar aspectos de Control de Ingreso, administración de los recursos y adicionalmente se recomienda realizar un cronograma de Visitas al Centro de datos, para comprobar la realización de pruebas para garantizar la Seguridad de los Servidores y de manera especial la Información que se encuentra distribuida en la Base de Datos.

ASAPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		función a la realidad del ambiente. 2. Formalización / Estandarización.	
Al igual que es necesario mantener un inventario de Activos de Información por las razones antes expuestas; es necesario también mantener un inventario de activos de TI en donde se especifique el detalle de hardware, software, aplicaciones y licencias. De la revisión de la documentación alcanzada se ha identificado que se tiene un inventario de aplicaciones y	Al no tener un inventario de activos de TI la administración de la "hoja de vida" sobre los activos de TI se vuelve más complicada, tanto para su identificación como para el control y seguimiento. A través de esta "hoja de vida", se podrá asociar los activos con los incidentes reportados sobre éstos	Realizar un inventario de activos de TI o de Elementos de Configuración (CI: Configuration Item) por jerarquías o grados de profundidad en donde se tenga información sobre sus atributos (físicos, pertenencia, ubicación, etc.) y la relación entre los mismos.	Se reitera la recomendación que es muy necesario el inventario de activos de TI y los elementos que lo conforman, para mantener información sobre las características y propiedades de cada ítem, para conocer su emplazamiento, pertenencia, número de serie y la clasificación de Seguridad que es necesario, por lo expuesto en Seguridad.

ASAPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
licencias al 19/11/2008 en donde se especifica software de ofimática principalmente (Office XP Small Business, Office 2003, Visio y Project); sin embargo este inventario no refleja atributos adicionales tales como relación entre los mismos, ubicación, etc.; guardando detalles actuales e históricos sobre los estados durante el ciclo de vida.	y, de esta manera, poder realizar análisis de problemas sobre una base estadísticas de incidentes más recurrentes sobre un grupo particular de activos.	Beneficios: 1. Permite asociar incidentes sobre un activo específico, con lo cual se puede extraer información sobre activos afectados y tendencias. 2. Mejora la precisión en la gestión de cambios y facilita la gestión de riesgos 3. Las relaciones entre Activos de Información son útiles para diagnosticar errores y predecir la disponibilidad de los servicios; (i) Físicas: Forma	Los beneficios son los mismos expuestos en nuestras recomendaciones del año 2009.

ASAPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		parte de, está conectado a, es necesario para, y (ii) Lógica: Es copia de, se relaciona con, es usado por. 4. Mejora el control del hardware y el software.	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
A pesar que existe un formato para la solicitud de requerimientos de sistemas para nuevas funcionalidades y/o proyectos, según las encuestas aplicadas a los usuarios claves, éste no se aplica de acuerdo a lo especificado. No se ha logrado aún estandarizar la canalización de requerimientos; los usuarios no tienen una forma estándar de solicitar sus requerimientos; las solicitudes se hacen a través del formato, a través de correo electrónico o por teléfono. Asimismo, a través de las entrevistas con los usuarios, se percibe un distanciamiento entre el área de TI y sus clientes (usuarios).	Un formato de solicitud de requerimientos debe permitir al usuario canalizar sus necesidades al área de sistemas y debe ser el primer input de información con lo cual el área de sistemas pueda interpretar la necesidad. Sin embargo, el formato debe ser un primer input de información del requerimiento; información que debe ser complementada en las etapas sucesivas con información adicional que le dé al usuario y al equipo de sistemas información sobre el avance de la	Realizar mejoras a los procedimientos de Requerimiento de Sistemas en donde se considere una clasificación por prioridad (cambios de emergencia, cambios urgentes, cambios de prioridad normal, cambios de baja prioridad) e impacto (impacto menor, impacto sustancial, impacto mayor). El formato de requerimientos debe estar alineados a los procedimientos y permitir al usuario y al personal de sistemas registrar la	Las solicitudes debidamente establecidas mediante un formato establecido, son revisadas por el Comité de Sistemas, Comité de Negocios y el Comité SIAF, a través de los cuales se priorizan, se clasifican y se atienden de acuerdo a su grado de urgencia. Todos los requerimientos solicitados mediante el formato son atendidos, de acuerdo a su prioridad Considerar la implementación o desarrollo de una herramienta que permita el soporte de la administración de requerimientos.

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
	solicitud, estados, fechas, responsables, etc. De esta manera, el usuario se siente identificado con el servicio y el área de sistema mantiene control sobre la evolución de los requerimientos.	información relevante de la solicitud y la que se requiere controlar en las etapas de planificación, coordinación e implementación del cambio. Diseñar una fuente de información en donde se registre la información de los requerimientos que faciliten el seguimiento y la evaluación y que a su vez permita informar al usuario de manera ágil el estado de su solicitud, mejorando la comunicación en ambos sentidos.	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		Beneficios: 1. Evolución favorable de los sistemas al estar el usuario conectado e identificado con sus requerimientos. 2. Revisar los procedimientos de comunicación con el usuario (el de solicitud de requerimientos en uno de ellos) es un claro mensaje de la orientación del proveedor del servicio con su cliente. 3. Mejora la información administrativa sobre los	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		cambios, mejora el diagnóstico. 4. Mejora la flexibilidad de adaptación ante cambios de mayor impacto y de mayor prioridad; mediante un procedimiento conocido y aceptado por el usuario. 5. Una fuente de información facilita el control mediante indicadores de rendimiento del proceso.	
Actualmente se cuenta con 1 ambiente uno de producción en donde se encuentran los objetos organizados a	Al no tener centralizada la función de administración de fuentes para realizar el checkout y check in de	Asignar un responsable para administrar las fuentes en el ambiente de desarrollo, que sea	A la fecha, no se cuenta con un control centralizado de los programas fuente, lo cual puede

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
través de una librería independiente para GRELL y un ambiente de desarrollo y pruebas. El ambiente de producción es controlado y administrado por EL Jefa del Área de Computo. Los programas fuentes son administradas a través del Visual SourceSave; sin embargo, no existe una función centralizada para realizar el checkout y check in de los programas fuentes, por tanto estos programas fuentes pueden ser tomadas por cualquiera de los programadores del equipo asignado. Si bien el ambiente de producción es	los objetos en el Visual SourceSafe, existe un riesgo que se pierda el control de los cambios realizados en las fuentes de los programas y que los cambios no sean correctamente liberados al ambiente de producción. Asimismo, la toma de un objeto para que sea modificado debe necesariamente estar autorizada en función del cambio aprobado por el usuario y un análisis previo de los objetos que se requieren para aplicar el cambio solicitado. Es necesario llevar un registro de las últimas versiones de los objetos	quién libere los objetos mediante solicitudes aprobadas sustentadas por un análisis previo de tipo técnico. Complementar el Procedimiento de Pase a Producción con lo cual se reflejen los responsables del pase (coordinación, ejecución, aseguramiento y control); considerando una segregación de funciones entre el personal de desarrollo y el personal de producción. Evaluar la implementación de	conducir a errores significativos por el limitado control de versiones (por ejemplo: uso de versiones incorrectas o desactualizadas, modificación simultánea del mismo programa fuente por dos personas, entre otros casos). Actualmente cada Jefe de Proyecto de Sistemas es responsable por el control de los programas fuente. El ambiente de prueba está en proceso de implementación. Se sugiere evaluar, adicionalmente, la implementación de un ambiente de control de calidad.

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
administrado por el Jefe de Computo, la actualización de objetos para realizar los pases a producción es realizada tanto por el Jefe de Negocios TI como por una de los Analistas	con lo cual, en el momento de liberar a producción se asegure las liberaciones de las últimas versiones de aquellos objetos modificados producto de requerimientos aprobado. Es necesario que las liberaciones de objetos al ambiente de producción sea ejecutado por quien administra este ambiente, debidamente coordinado con los responsables de desarrollo; con lo cual se tenga una separación de ambientes (de desarrollo y producción) de manera física, lógica y funcional.	un ambiente de pruebas que simule el ambiente de producción en donde se puedan realizar las pruebas en un ambiente más estable que el actual. <u>Beneficios</u>: 1. Mejora las pruebas de los programas ante de la puesta en producción y reduce el riesgo de inestabilidad en los sistemas. 2. Mejor control en la administración y asignación de programas fuentes en la	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
	Carecer de un ambiente de pruebas, implica que las pruebas deben ser realizadas o en el ambiente de desarrollo (como actualmente se realiza) o en el ambiente de producción. Esta situación implica un riesgo al realizar el pase a producción puesto que las pruebas en un ambiente de desarrollo implica realizar pruebas en un ambiente "inestable"; entendiendo como tal a un ambiente que está siendo manipulado en alguno de sus objetos y no se puede simular con precisión la casuística de la	gestión de cambios. 3. Evita que el personal sea juez y parte ante la puesta en producción de programas y fortalece el control de los ambientes. 4. Formalización / Estandarización.	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
	funcionalidad modificada o de la nueva funcionalidad simulando situaciones reales. Esto conlleva en ocasiones activar procedimientos para revesar el cambio (back out) con lo cual se genera inestabilidad en el ambiente de producción lo cual puede afectar a varios usuarios.		
De la revisión del Contrato de Locación de Servicios celebrado en el mes de diciembre de 2008; se puede observar que no se detalla con precisión el alcance del servicio de TI ofrecido. Específicamente el Contrato de Locación	No contar con un catálogo de servicios detallado en el que se especifique como mínimo las necesidades del cliente por los servicios contratados, acuerdos de niveles de servicio, tiempos de respuesta y esquema de monitoreo	Revisar el Contrato de Servicios Informáticos y detallar mediante un catálogo de servicios los acuerdos de niveles de servicio que permitan evaluar el servicio proveído.	A la fecha no se cuenta con un catálogo de los acuerdos de niveles de servicios, ni se cuenta con una persona para realizar la evaluación del cumplimiento de estos niveles de servicio.

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
de Servicios indica en su segunda cláusula: "*Por el presente contrato, La Locadora se obliga a prestar entre otros, los servicios de Cobranzas, Compras, Seguridad, Suministros, Contabilidad, Recursos Humanos, Fotocopiado, Mensajería, Central Telefónica y Sistemas en el Uso, Desarrollo y Mantenimiento de Aplicaciones, Uso del Servidor, Sistemas de la institución Operaciones por Internet, Centrales y Gestión de Proyectos Informáticos, así como cualquier otro servicio que resulte necesario para La Comitente".* Como se observa en la segunda cláusula del contrato no se especifica de manera	y evaluación del servicio dificulta controlar el servicio de TI que se recibe; con lo cual se pueda identificar ajustes en el servicio necesarios para mejorar permanentemente el servicio recibido.	Asimismo, se sugiere asignar un responsable que evalúe el servicio de TI, que emita reportes de desempeño en función de métricas objetivas a la Alta Dirección de GRELL. En concreto el SLA: – Es un acuerdo escrito entre la organización TI y el cliente – Describe los detalles en términos cuantitativos (métrica) de los servicios a ser proporcionados – Describe los servicios en	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
detallada los servicios de TI ofrecidos, los acuerdos de niveles de servicio establecidos, tiempos de respuesta, esquema de monitoreo y seguimiento a los servicios, entregables, etc.		términos no técnicos Beneficios: 1. Mantener y mejorar la calidad del servicio TI, a través de un ciclo constante, que involucra: abordar, monitorear, generar reportes y revisar mejoras del servicio TI.	
Tal como se menciona en el Plan Estratégico de enero de 2009, uno de los objetivos estratégicos del negocio es "*intensificar el uso del SIAF*", lo cual permite reducir considerablemente los tiempos de ciclo para las operaciones tanto	Caídas constantes en los SERVIDORES implica cerrar un canal de atención que tiene un impacto directo en el cliente; un impacto tanto en la operatividad del negocio como en la	Las caídas del SERVIDORES más que incidentes se deben de considerar como un problema (entiéndase como problema a "*una condición identificada como resultado de múltiples*	El Sistemas de la institución, está en continuo mejoramiento. Se han revisado las causas que producían los problemas identificados en la Auditoria 2009. La solución adoptada le ha permitido al

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
de ingresos y liberaciones. El SIAF, desde su lanzamiento ha evolucionado favorablemente desde el punto de vista funcional, sin embargo falla desde el punto de vista de disponibilidad. El usuario principal responsable del desarrollo SIAF ha registrado 13 incidentes en el periodo comprendido del 15 de junio al 7 de julio (17 días útiles) que impide al usuario realizar operaciones (no se tiene registro sobre incidentes anteriores).	percepción de la efectividad del SERVIDORES para sostener una estrategia institucional que requiere de la aceptación de agentes externos a GRELL. Si bien el SERVIDORES ha demostrado que logra reducir considerablemente los tiempos de ciclo, no tener controlado la disponibilidad del servicio pone en riesgo la sostenibilidad de la solución, le resta competitividad contra la solución alternativa de la competencia , pone en riesgo la implementación de una estrategia institucional que responde a una	*incidentes que exhiben síntomas comunes*" según como lo denomina ITIL). En tal sentido, se sugiere realizar un análisis de causas (puede haber más de una) detallado de las caídas que se presentan en el sistemas de la institución y atacar el problema desde la raíz del problema para brindar una solución estructural. Se sugiere también, tratar de identificar y documentar workarounds para errores conocidos que faciliten el restablecimiento del servicio en	Usuario Final, (Cliente), mejorar la disponibilidad, acceso y explotación de la información.

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
	tendencia del mercado.	el menor costo posible. La documentación en este caso es importante, debido a que se trata de un servicio crítico que debe poder ser levantado en un corto tiempo independiente de las personas disponibles en el momento que se produce la caída. <u>Beneficios</u>: 1. Definir y documentar workarounds reducen el tiempo en el que se levanta el servicio por "errores conocidos".	

ASPECTOS DE LA ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		2. Atacar las diferentes causas reducen considerablemente a la ocurrencia de un número elevado de incidentes y el impacto es percibido inmediatamente por el cliente (usuario).	

ASPECTOS DE LOS PROCEDIMIENTOS DE RESPALDO			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
GRELL sistemas tiene implementando un procedimiento de backup de información, el cual se realiza con las frecuencia y alcance necesario. Según el jefe de sistemas, cuando ha sido necesario restaurar información de los backups el procedimiento ha sido aplicado con éxito; sin embargo, lo que no hay evidencia es que se realicen pruebas de restauración de información crítica para asegurar la aplicación de los procedimientos y un conocimiento extensivo del personal involucrado para su aplicación.	Además de tener los procedimientos documentados, es importante que los procedimientos sean conocidos por las personas involucradas para su ejecución. El procedimiento de restauración, por ser un procedimiento de contingencia, su ejecución se realiza de manera extraordinaria y un buen entrenamiento contribuye al éxito de su ejecución cuando es requerido.	Es importante realizar chequeos sobre los procedimientos de respaldo con determinada frecuencia y de manera sorpresiva. Estos chequeos deben estar orientados a simular la restauración parcial y total de la información crítica del negocio. Beneficios: 1. Aseguramiento por parte del negocio que los procedimientos de respaldo funcionan correctamente y el	Se recomienda revisar servicios ofrecido por el Ministerio, en el Data Center, que debe considerar aspectos sobre los Procedimientos de Respaldo, que satisfagan la necesidad de Servicio de la institución, como la información diaria, semanal, mensual e histórica. Se recomienda realizar un cronograma de Visitas al Ministerio, para comprobar la realización de pruebas de backups orientadas a simular la restauración parcial y total de la información crítica del negocio.

ASPECTOS DE LOS PROCEDIMIENTOS DE RESPALDO			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
	Asimismo, las pruebas de backups son importantes para verificar que los datos almacenados estén completos, estén bien guardados (sin errores). Asimismo, es importante verificar el tiempo de vida de los medios de almacenamiento para asegurar que no se presenten fallas en la restauración originados por problemas del medio de almacenamiento.	Equipo de Software y Aplicaciones de Negocio están entrenados para recuperar la información en periodo oportuno bajo situaciones de alto stress.	

ASPECTOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
El documento 1.12 Políticas y Procedimientos incluye una sección de Recuperación de Desastres y Continuidad de Negocio; asimismo, ha sido revisado el documento Plan de Continuidad de Negocio donde se identifica los procesos críticos identificados por GRELL Sin embargo, en ninguno de los documentos se contempla la totalidad de los temas requeridos por la norma: 1. Entendimiento de la Organización: Donde se define un (i) Análisis de Impacto para determinar el impacto de una interrupción de los procesos de TI que soportan al negocio; y un (ii) Análisis de Riesgos para determinar los riesgos que podrían	Sin un Plan Estratégico de Tecnología de Información formalmente desarrollado, existe el riesgo se definan estrategias de continuidad que impliquen destinar esfuerzos en la implementación de controles para recuperar operaciones del negocio que no se ajusten completamente con los requerimientos de mediano y largo plazo. Asimismo, si bien existe una buena base del Plan de Continuidad de Negocio, aún	Revisar de manera detallada el Plan de Continuidad de Negocio y determinar el alcance de su aplicación para las operaciones de la institución. En base a esta referencia, se sugiere actualizar el Plan de Continuidad de Negocio; bajo responsabilidad de las áreas de negocio en coordinación con el área de sistemas. Es importante, que la elaboración y actualización del Plan de Continuidad de Negocio	El nuevo servicio ofrecido por MINISTERIO del Perú, en el Data Center, debe considerar aspectos sobre la Continuidad de Negocio, para lo cual se hace necesario adecuar y sincronizar los Planes de Continuidad del Negocio de la institución con los de MINISTERIO, que deben estar enfocados a restablecer los Procesos Críticos del Negocio y a satisfacer lo dispuesto. Se sugiere desarrollar periódicamente prueba de los planes para verificar la efectividad y consistencia de los

ASPECTOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
interrumpir el negocio. 2. Selección de la Estrategia de Continuidad: Donde se seleccionan las estrategias de continuidad para los riesgos críticos 3. Plan de Crisis y Plan de Continuidad de Negocio 4. Plan de Pruebas y Actualización de los Planes	hay espacio para mejorar el documento y explotar la metodología utilizada para la complementar el Plan de Continuidad de Negocio.	responda a un análisis de los procesos críticos alineados al Plan Estratégico y al Plan Estratégicos de TI. En el documento 1.12 Políticas y Procedimientos se ha definido la Organización para la recuperación de desastres y se establecen responsabilidad. Se sugiere que de manera complementaria se desarrollen cartillas operativas donde se detalle a nivel individual para los miembros de cada equipo las actividades a realizar o checklist de actividades durante	mismos como caídas de tensión, pérdida del fluido eléctrico en las Instalaciones, fallas en la comunicación que MINISTERIO garantiza la Continuidad del Negocio, mediante sus Servidores Espejo (Mirrow).

ASPECTOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		la activación de los procesos de emergencia. Beneficios: 1. Más allá de desarrollar un documento de Plan de Continuidad de Negocio, el beneficio de hacerlo es reducir los riesgos de paralización de operaciones críticas con el consecuente impacto en el cliente; tanto de cobranzas, imagen, servicio, etc. 2. Identificación detallada de procesos de TI críticos	

ASPECTOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		alineados a los objetivos estratégicos, con el consecuente aseguramiento y protección del servicio. 3. Diseñar una cartilla ayuda al personal asignado a uno de los equipos de recuperación a actual de manera diligente en una situación de alta presión; donde la precisión en las actividades es crítica y el tiempo es un factor de stress adicional.	

ASPECTOS METODOLÓGICOS			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
El área de sistemas mantienen comités con las áreas de negocio en donde se revisa el avance de los proyectos y requerimientos, en donde se levanta un acta en donde se describe los Acuerdos Tomadas y se asignan responsables y fechas para las siguientes actividades. Sin embargo, de acuerdo al Jefe de Sistemas, no existe una aplicación exhaustiva de técnicas de gestión de proyectos que permita documentar el proyecto, identificar las desviaciones en la planificación, gestionar los riesgos del proyecto, medir los costos, etc.	Aplicar parcialmente técnicas de gestión de proyectos pone en riesgo al proyecto en sí; aumenta las probabilidades de error en alguno de las áreas del proyecto (integración, alcance, tiempo, costo, riesgos etc.) con lo cual se pueden presentar desviaciones en algunas de las fases del proyecto.	Hay que considerar que un proyecto no es el fin en sí mismo sino un medio para aplicar una estrategia específica. En tal sentido, la misión del Gerente de Proyecto es alcanzar el objetivo deseado según las definiciones del negocio considerando tiempo, costos y calidad. Tomando en cuenta la definición anterior, se sugiere formalizar una metodología para la gestión de proyectos con lo cual se pueda controlar con mayor precisión el avance y la	A la fecha no se cuenta con la Metodología de Gestión de Proyectos recomendada en la Auditoria 2009. Adicionalmente se puede mencionar que la Gerencia de TI no cuenta con una herramienta que le permita Controlar efectivamente sus proyectos, para determinar el grado de avance, objetivos parciales alcanzados, costos, entre otros aspectos. Actualmente cada Jefe de Proyecto controla sus proyectos con herramientas como el MS

ASPECTOS METODOLÓGICOS			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		medición de los resultados. La metodología más difundida de gestión de proyecto es la PMBOK difundida por el PMI, esta aborda la gestión de proyectos en diferentes áreas de conocimiento y proporciona buenas prácticas en cada una de éstas. Se sugiere revisar en detalle esta metodología y adecuarla a las necesidades de la institución para su formalización. <u>Beneficios</u>: 1. Mejorar la gestión de	Project, que brinda facilidades de control en lo que respecta al cumplimiento de las actividades y el rol de los responsables. Se recomienda evaluar el uso de una herramienta integrada para el control de proyectos que facilite la aplicación de la metodología.

ASPECTOS METODOLÓGICOS			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
		proyectos y contribuir para que éstos cumplan los objetivos de tiempo, costos y calidad.	

ASPECTO DE PLANIFICACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
El área de sistemas de GRELL no cuenta con un Plan Estratégico de Tecnología de Información que marque la tendencia tecnológica de mediano y largo plazo de acuerdo al Plan Estratégico de GRELL (estrategias de hardware, software, comunicaciones y personal).	Sin un Plan Estratégico de Tecnología de Información no se puede establecer con claridad cuál es el rumbo donde se debe alinear las actividades de TI, y para GRELL resultaría más complejo hacer un seguimiento como usuario del servicio de TI. No tener una Plan Estratégico de TI impide medir la performance del servicio de TI y evaluar los logros obtenidos. En base a este plan se deben elaborar otros planes, tales como el plan de capacitación, plan de	Desarrollar el Plan Estratégico de Información en coordinación con el área de sistemas de GRELL y las áreas de negocio y establecer los procedimientos para actualización y revisión anual. <u>Beneficios</u>: 1. Sustentar las actividades de sistemas sobre la base de un Plan Estratégico de Tecnologías de Información facilita que los esfuerzos de sistemas en cada uno de sus frentes estén alineados con	Aún no se cuenta con un Plan Estratégico de Tecnología de Información que marque la tendencia tecnológica de mediano y largo plazo de acuerdo al Plan Estratégico de GRELL (estrategias de hardware, software, comunicaciones y personal). El Usuario responsable manifestó que mediante la Reorganización del Grupo en el Primer Trimestre del año 2012, se tendrán resultados. La Unidad de TI, ha

ASPECTO DE PLANIFICACIÓN			
SITUACIÓN ACTUAL	**RIESGO ASOCIADO**	**RECOMENDACIONES 2009**	**ESTADO AL 2013**
	adquisición de recursos y contratación de servicios, plan de continuidad de negocio, plan de seguridad de información, entre otros.	las estrategias del negocio y a través de sus seguimiento y monitoreo de resultados permite identificar desviaciones en su ejecución; asegurando un adecuado soporte al negocio por parte, tanto por las aplicaciones como por la organización y estructura del área sistemas responsable de proveer el servicio.	presentado un Plan Estratégico primario que debe actualizarse, para alinear con los cambios de ubicación de Servidores, Sistema de Seguridad de Información, Sistema de Respaldo, entre otros.

2.3.8 CONCLUSIONES DE LA AUDITORIA

A continuación se listan de manera resumidas las recomendaciones realizadas a lo largo del presente informe. Es importante mencionar que se deberá evaluar cada una de estas recomendaciones y, en función del apetito de riesgo de la institución, realizar un plan para su atención tomando en cuenta variables como impacto en el negocio, importancia, urgencia, esfuerzo de la implementación, entre otras.

1. Desarrollar la funcionalidad que actualmente no está soportada por los Sistemas de Información, en base a un estudio integral de requerimientos.

2. Revisar el procedimiento de contratación de servicios con terceros que afecten servicios de TI en que se considere un análisis de riesgo previo por cambios de proveedores o cambios en el alcance del servicio.

3. La organización no tiene un IHTI detallado ni en unidades ni en valores. No se conserva adecuadamente los equipos fuera de uso, provocando que se deterioren y ya no sirvan.

4. La organización no tiene un Plan Estratégico.

5. No se prueba el Plan de Continuidad del negocio.

6. Comúnmente es confundido con el Plan de Contingencia Informática.

7. La organización no tiene un Plan de Seguridad de la Información.

8. Las claves de seguridad de acceso a diversas tecnologías de la información son conocidas por personas que no necesitan saberlo o son cambiadas sin notificar al jefe encargado de ello.

9. Errores en la seguridad física:

   Los extinguidores de incendios no son apropiados para apagar incendios de equipos electrónicos. Ej.: extinguidores de chorro de agua en lugar de extinguidores de dióxido de carbono o polvo químico seco.

Existencia de material inflamable como cuadernos, papeles, madera, etc.

10. La reestructuración de la Institución La Gerencia Regional de Educación La Libertad es una ventaja competitiva que de seguro permitirá el desarrollo de los Planes en el que se incluye el Plan Estratégico de Tecnologías de Información, Plan de Seguridad de Información, Plan de Continuidad de Negocio, entre otros.

11. Hay diferencias en los modelos de estaciones de trabajo instaladas, debido al cual en algunas estaciones se percibe mayor lentitud durante las consultas y procesos que en algunas otras hay respuestas óptimas, ejemplo (PC´s de Inspectoría, lentas, vs PC´s de Negocios, más rápidas).

12. Desarrollar la funcionalidad que actualmente no está soportada por los Sistemas de Información, en base a un estudio integral de requerimientos.

Capítulo III: PLAN DE MEJORA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD

3. SGSI Y PCN

3.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Después de realizar la auditoria a la GRELL, la alternativa que se plantea, es seguir un Sistema de Gestión de Seguridad de la Información.

¿Y por qué implantar un SGSI?

Porque un SGSI permite dotar y mantener seguridad, sobre la información que maneja la organización. Si además se certifica con el estándar ISO/IEC 27001, ofrece una ventaja competitiva.

La certificación ISO/IEC 27001 demuestra:

- El cumplimiento de requisitos para la gestión corporativa y la continuidad del negocio.
- El valor que tiene la seguridad de la información para la organización debido al compromiso de la cúpula directiva.
- La garantía de controles externos a la propia organización.
- Que los riesgos de la organización están identificados, evaluados y controlados.
- El cumplimiento de leyes y normativas que sean de aplicación.
- La mejora continua consecuencia de las revisiones periódicas.

El SGSI se basa en un conjunto de políticas orientadas a conseguir y a mantener la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la Información.

3.1.1 OBJETIVOS

1) Implementar un Plan de Mejora de un Sistema de Gestión de Seguridad de Información y Continuidad, bajo lineamientos y buenas prácticas:

   a. ISO 27001. Sistema de Gestión de Seguridad de la Información
   b. COBIT 4.0Buenas prácticas

2) Presentar el resultado del diagnóstico de las actividades de Gerencia Regional de Educación La Libertad.

3) Identificar las brechas y proponer acciones para cubrirlas a fin de lograr implementar efectivamente un Sistema de Gestión Seguridad de la Información.

4) Identificar la documentación necesaria que debe adecuarse o elaborarse para cumplir con los requisitos de las normas.

3.1.2 ALCANCE DEL DIAGNOSTICO SITUACIONAL INICIAL

1. El alcance del diagnóstico está referido a las actividades en las instalaciones de Gerencia Regional de Educación La Libertad.
2. El alcance incluye la identificación de procesos, evaluación de la documentación existente y el grado de implementación de los requisitos de la normatividad mencionada.

3.1.3 METODOLOGÍA

Se visitó, entrevisto y se hizo encuestas al personal de las instalaciones de la institución GRELL el día 21 de enero de 2013, en horas de la mañana, realizándose las siguientes acciones:

1. ENTREVISTA AL PERSONAL

   Se entrevistó a la Jefa de Computo, previa coordinación.

2. REVISIÓN DE LA DOCUMENTACIÓN

Se solicitó la documentación existente en la institución relacionadas a las normas.

3. EVALUACIÓN “IN SITU”

Se basó en conversaciones con el entrevistado y el recorrido a las áreas de: Área de Cómputo y Centro de Datos

4. COMPROMISO DE CONFIDENCIALIDAD

El consultor/auditor externo se compromete a mantener absoluta reserva de la información proporcionada por GRELL

3.1.4 DIAGNOSTICO SITUACIONAL INICIAL

De manera general, como resultado de la visita a las instalaciones, se encontraron las siguientes observaciones:

1. DOCUMENTACIÓN DE LA EMPRESA:
    a. No existen políticas de seguridad de la Información.
    b. No existe documentación de procesos.
    c. No existe documentación de continuidad del centro de datos.
    d. Objetivos de empresa de manera informal.
    e. Falta de identificación formal de requisitos del cliente.
    f. No existen plan de capacitación establecido.

2. CONTROLES OPERACIONALES
    a. No existen acciones asociadas a la normativa 27001
    b. Falta de delimitación de área.
    c. Falta de identificación de peligros y evaluación de peligros.
    d. Desconocimiento del impacto operacional de la institución.
    f. No se cuenta con procedimientos operaciones ni controles.
    g. No existe registro de accidentes.
    h. No se tiene definido qué situaciones merecen dar origen a acciones correctivas, preventivas y de mejora y cómo tratar cada una de ellas.

Como resultado de la evaluación documentaria se ha considerado necesario

elaborar la siguiente estructura documentaria como base necesaria para sustentar el PLAN DE MEJORA:

- Manual de Gestión en Seguridad de la Información
- Procedimientos Generales y Específicos
- Manual de Continuidad del Centro de Datos
- Registros asociados a los procedimientos

Adicionalmente, se determinará la documentación necesaria en función a la complejidad de los procesos de GRELL y la competencia del personal

3.1.5 TIEMPO DE IMPLEMENTACIÓN

1. Se considerará un tiempo estimado de 4 meses.
2. Existen factores a considerar dentro de la implementación del SGSI:
    a. Experiencia y/o cultura de gestión
    b. Recursos internos
    c. Competencia del personal
    d. Exigencia corporativa
    e. Generación de la documentación
    f. Auditorías internas
    g. Identificación de peligros y evaluación de riesgos
    h. Identificación de aspectos ambientales significativos

3.1.6 CRONOGRAMA DE ACTIVIDADES

ETAPAS	ACTIVIDADES	Jun-13			Jul-13				Ago-13				Oct-13					Nov-13				Dic
Diagnostico	Diagnostico Situacional inicial																					
	Presentación de propuesta																					
Planeación	Caracterizar la organización																					
	Elaborar políticas																					
	Elaborar FODA de la organización																					
Diseño	Estructurar la empresa por procesos																					
	Definir la estructura organizativa en el SGSI																					
	Asignar responsabilidades y autoridades																					
	Definir el alcance y las conclusiones del SGSI																					
	Definir indicadores de desempeño en el SGSI																					
	Objetivos Integrales - Metas Integrales																					
	Elaborar documentación del Sistema																					
Implementación	Definir el programa de implementación del SGSI																					
	Divulgación del SGSI a todos los niveles																					
Verificación	Realizar auditorías internas																					
	Acciones de mejora																					
	Medición del desempeño por indicadores																					
Mejora Continua	Revisión por la Dirección																					
	Revisar cumplimiento de objetivos																					
	Mantenimiento y mejora del SGSI																					

3.1.7 FASES Y ACTIVIDADES

La alta gerencia es la responsable del proyecto de implantación. Se debe asignar a un gerente (nivel táctico) de la organización la responsabilidad de la gestión del proyecto y sus actividades. Este gerente estará controlando el avance de las fases del ciclo y el consumo de recursos. En esta etapa es importante decidir quién tendrá, a lo largo del proyecto de implantación, la responsabilidad por la documentación del modelo.

3.1.7.1 FASE 1 TALLER ESTRATÉGICO CON LA GERENCIA PARA ANALIZAR REQUERIMIENTOS

Esta fase es fundamental; tanto los niveles estratégicos como los tácticos en la organización deben entender los requerimientos de la norma y la lógica del funcionamiento del SGSI, así como sus beneficios.

3.1.7.2 FASE 2 DETERMINACIÓN DEL ALCANCE

El ISO 27001:2005 está concebido bajo la óptica de sistemas. Vale decir, lo que se aplica al todo puede aplicarse a cada elemento del todo. La amplitud del alcance en una empresa dependerá de muchos factores. Uno de ellos serán los recursos disponibles, la experiencia en la implantación y la criticidad de algunos procesos en relación con el riesgo de información. Por lo general, la implantación del modelo se realiza por procesos, que se han considerado críticos, por su exposición al riesgo y el impacto en la competitividad de la firma. Cuando es la primera vez que se desea implantar el modelo en una empresa, no se debe ser tan ambicioso y escoger un proceso muy complejo que pudiera hacer fracasar la implantación.

La definición del alcance, obedece a 2 etapas: la primera es la estratégica, y la otra táctica, que es la netamente técnica.

Etapa estratégica para determinar el alcance del modelo

Esta etapa está dirigida a resolver la pregunta ¿Cuál o cuáles procesos son los

candidatos para implantar el modelo?

Esta etapa consiste en identificar los “factores críticos del éxito” de la empresa y, por otro lado, identificar los procesos críticos de la organización.

Etapa táctica para determinar el alcance del modelo

La etapa táctica consiste en aplicarles a los procesos identificados en la etapa estratégica.

Conviene tener en cuenta que la ejecución de las etapas estratégica y táctica para determinar el alcance debe ser realizada por grupos multidisciplinarios, compuestos por representantes de los procesos organizacionales que se están analizando. Esto es vital, porque sólo los responsables del proceso son los que más conocimientos tienen sobre la problemática y la naturaleza de su proceso.

Además, hay6 algo muy importante: la dinámica de grupo que se va desarrollando a lo largo de la metodología de implantación hace que se genere un espíritu de equipo, el cual facilita de manera significativa la implantación y la aceptación del modelo en la firma.

3.1.7.3 FASE 3 - EFECTUAR UN ANALISIS Y EVALUACIÓN DE RIESGO

En esta fase los aspectos que deben lograrse son la identificación detallada de todos los activos de información, comprendidos en el alcance del modelo de la empresa. En seguida, para conocer el impacto de cada activo de información en la organización, se debe tasar cada activo con base en su confidencialidad, integridad y disponibilidad. Una vez efectuada la tasación, la empresa decidirá cuales son aquellos activos de información considerados importantes.

El paso que se debe de seguir es iniciar el análisis de riesgo para concluir con un estimado de riesgo por cada activo de información. A los activos de información que como resultado del análisis de riesgo se les considere más críticos, se les efectuará una evaluación de riesgo. El resultado de esa evaluación es identificar aquellos activos de información más significativos. Se recomienda utilizar COBIT para análisis de riesgo.

Una vez concluidos el análisis y la evaluación del riesgo, es el momento más propicio para redactar la política y los objetivos de seguridad de información.

3.1.7.4 FASE 4 – ELABORACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO

La secuencia metodológica de un plan de continuidad del negocio está redactada con el detalle necesario en el capítulo 4. Todos los componentes de la metodología cumplen con las actividades de esta fase.

Esta fase de elaborar un plan de continuidad del negocio, sea ubicado en esta parte del método, pues usualmente el lead time del proyecto de implantación viene determinado por el plan de continuidad del negocio.

3.1.7.5 FASE 5 – IMPLEMENTAR Y OPERAR EL SGSI

Esta fase se ha dividido en las actividades siguientes, explicadas a continuación.

Elaborar el plan de tratamiento del riesgo. Utilizando como insumos las decisiones de las opciones para el tratamiento del riesgo y la selección de los controles y objetivos de control a implantar, se debe elaborar el plan de tratamiento del riesgo. Este plan es una pormenorización de las responsabilidades, los recursos, tiempos y mecanismos de control para implantar las estrategias escogidas de tratamiento del riesgo. Se recomienda utilizar COBIT en este punto.

Determinar la efectividad de los controles y la métrica. Aquí se debe determinar la métrica que se utilizará para identificar la efectividad de los controles seleccionados, y que también definir cómo se va a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles.

3.1.7.6 FASE 6 – MONITOREAR Y REVISAR EL SGSI

Una vez el modelo esté funcionando en la institución/empresa, es necesario haber diseñado los mecanismos para monitorear y revisar su desempeño, y poder

cerciorarse de que el SGSI opera como estaba planeado. Las actividades de esta fase son las siguientes:

Detección de incidentes y eventos de seguridad. La organización debe tener los procedimientos respectivos para poder rápidamente reportar incidentes de seguridad y detectar los eventos de seguridad, tomar acciones y evitar que se conviertan en incidentes de seguridad.

Realización de las revisiones periódicas al SGSI. Se deben desarrollar los procedimientos que aseguren que, de manera periódica, se revisa el funcionamiento del SGSI y se verifica la efectividad de los controles instaurados.

3.1.7.7 FASE 7 – MANTENER Y MEJORAR EL SGSI

En esta fase se deben establecer los mecanismos que permitan generar la evidencia objetiva de que el SGSI se mantiene y se mejora constantemente.

Implementar las acciones correctivas y preventivas. Se deben tener los respectivos procedimientos documentados (exigencias de la norma), y haber generado en la cultura de la organización el hábito de que, antes un no cumplimiento de requerimientos (no conformidad), se generen acciones correctivas. Por otro lado, la empresa debe haber desarrollado el hábito de estar periódicamente revisando estadísticas, observar tendencias y, con base en esa información, elaborar acciones preventivas.

3.1.7.8 FASE 8 – DESARROLLO DE COMPETENCIAS ORGANIZACIONALES

En esencia, se requieren tres competencias básicas, las cuales conforman las tres actividades de esta fase:

Entrenamiento en documentación de un SGSI. Es de vital importancia que el personal afectado por la implantación del modelo tenga destrezas para poder documentar procedimientos, políticas, instrucciones de trabajo, y saber identificar registros del Sistema de Seguridad de Información. Un entrenamiento

formal es importante. Quizás esta actividad debiera ejecutarse al inicio del proyecto.

Entrenamiento en manejo de acción correctiva y preventiva. Ante la ocurrencia de una no conformidad (el no cumplimiento con los requerimientos) se debe iniciar la acción correctiva. El objetivo de este requerimiento es que, con base en evidencias objetivas de ocurrencias, se vean las tendencias y la empresa desarrolle acciones preventivas para evitar que la no conformidad se presente. Es de suma importancia que el personal en la empresa conozca la metodología y las herramientas para el correcto manejo de la acción correctiva y preventiva.

Entrenamiento en manejo de auditoría interna. La auditoría interna, tal como exige la cláusula 6 de la norma, requiere que la empresa se audite a sí misma para demostrar que su sistema se mantiene y que busca nuevas oportunidades de mejora.

3.1.7.9 FASE 9 – REDACCIÓN DEL MANUAL DE SEGURIDAD DE INFORMACIÓN

La actividad básica de esta fase es la redacción del Manual de Seguridad de Información

3.1.7.10 FASE 10 – EJECUCIÓN DE AUDITORIAS INTERNAS

Para poder cumplir con los requerimientos de las auditorías internas, ellas deben llevarse a cabo cumpliendo todas las exigencias de la cláusula 6 de la norma. En una práctica internacional que, en 12 meses, la empresa haya auditado la implantación de todas las cláusulas de la norma.

Realización de las auditorías internas. La empresa debe haber decidido si las auditorías internas serán subcontratadas o realizadas por personal interno. Bien sea una u otra opción, las auditorías deben realizarse cumpliendo con todas las exigencias de la cláusula 6 de la norma, y utilizando el lineamiento ISO 19011:2002.

3.1.7.11 FASE 11 – OBTENCIÓN DE LA CERTIFICACIÓN INTERNACIONAL

FASES	ACTIVIDADES
I. Entendimiento de los requerimientos del modelo	1. Taller con niveles estratégicos y tácticos
II. Determinación del Alcance	2.Etapa estratégica 3. Etapa Táctica
III. Análisis y Evaluación del riesgo	4. Realización del análisis y evaluación del riesgo. 5.Definición de política de seguridad de información y objetivos 6. Evaluación de las opciones para el tratamiento del riesgo 7. Selección de controles y objetivos de control. 8. Evaluación de la declaración de aplicabilidad.
IV. Elaboración del plan de continuidad del negocio	9.Realizar el Business Impact Analysis 10. Efectuar el análisis del riesgo e identificar escenarios de amenazas. 11. Elaborar estrategias de continuidad. 12. Diseñar plan de reanudación de operaciones 13. Diseñar procesos de ensayos
V. Implementar y operar el SGSI	14. Elaborar el plan de tratamiento del riesgo. 15. Determinar la efectividad de los controles y las métricas
VI. Monitorear y revisar el SGSI	16. Detección de incidentes y eventos de seguridad. 17. Realización de revisiones periódicas al SGSI.
VII. Mantener y mejorar el SGSI	18. Implementar las acciones correctivas y preventivas.

VIII. Desarrollo de competencias organizacionales	19. Entrenamiento en documentación del SGSI. 20. Entrenamiento en manejo de la acción correctiva y preventiva. 21. Entrenamiento en manejo de auditoría interna.
IX. Redacción del Manual de Seguridad de Información	22. Redacción de las auditorías internas
X. Ejecución de las auditorías internas	23. Realización de las auditorías internas
XI. Obtención de la certificación internacional.	24. Búsqueda de la empresa certificadora. 25. Realización de la auditoria por parte de la certificadora. 26. Obtención de la certificación

3.1.8 CONSIDERACIONES A LA IMPLEMENTACIÓN DEL SGSI

1. **Beneficios potenciales de un SGSI.**
   - Mejora la organización y asignación de responsabilidades en lo relativo a seguridad de la información de la empresa.
   - Permite documentar y estandarizar las actividades referentes a la gestión de la seguridad de la información
   - Disminuye el riesgo del posible uso de información confidencial por parte de personal ajeno.
   - Conseguir un sistema que aprenda de los errores y que evolucione constantemente.
   - Involucrar al personal como parte activa y creativa en el proyecto.
   - Aumenta la rentabilidad a mediano y corto plazo, al disminuir la probabilidad de pérdida y fuga de información de la institución

2. **Racionalización de los recursos.**

   La implantación de un SGSI permite la racionalización de recursos, ajustando las inversiones en tecnología a las prioridades impuestas a través del Análisis de Riesgos, evitando así gastos innecesarios,

inesperados y sobredimensionados.

3. Reducción de riesgos

Mediante la implantación de controles, se garantiza la continuidad del negocio frente a las amenazas y vulnerabilidades.

5. Integra la seguridad en la gestión de la empresa:

Deja de lado un conjunto de actividades técnicas más o menos organizadas, para transformarse en un ciclo de vida metódico y controlado.

6. Cumplimiento legal

Los aspectos de conformidades legales de la norma exigen la verificación, la adecuación y cumplimiento de la legislación del país, en concreto, protección de datos, propiedad intelectual, servicios de la sociedad de la información y comercio electrónico, etc.

3.1.9 DIFICULTADES DE UN SGSI

1. Falta de Compromiso de la Alta Gerencia

El estándar ISO/IEC 27001:2005 es un documento que principalmente establece la necesidad de compromiso por parte de la Alta Dirección para la adecuada definición de Alcance, Limitaciones, definición de los Roles y Responsabilidades en materia de seguridad y la Asignación de los Recursos requeridos. La formación, toma de conciencia y competencia del personal son otras responsabilidades de la Alta Dirección, junto con la participación en la revisión de la eficacia y eficiencia del Sistema de Gestión implantado. Todos estos aspectos en muchos casos, son difíciles de encontrar en las empresas.

2. **Ausencia de una adecuada Gestión de Riesgo**

Otro tema fundamental al momento de implementar un Sistema de Gestión de la Seguridad es conocer los riesgos a los cuales se encuentra expuesta la Organización, y a través del análisis de los mismos establecer el tratamiento que se considere el más adecuado. Si bien es uno de los requisitos del estándar, es poco frecuente encontrar que hayan realizado alguna vez un análisis de riesgos. En algunos se encuentra por el tipo de actividad de la Organización, pero en muchos otros casos no se realiza. También se pueden encontrar casos en donde la Organización describe un "análisis de riesgos" y en realidad sólo han evaluado subjetivamente algunas pocas amenazas sobre los activos que más conocen, sin tener una idea clara de su valor y por otro lado sin conformar la totalidad de los activos de la Organización o al menos del proceso evaluado.

3. **Debilidades en la Gestión de Activos**

Un aspecto que resulta clave al momento de implantar un SGSI es el referido a los Activos de Información y el tratamiento que la Organización le da a los mismos. En principio el factor principal es contar con los activos de información más relevantes (o al menos los incluidos en el proceso que queramos analizar), algo que no es fácil de lograr y que en pocas ocasiones se encuentra. En algunos casos no existe tal inventario o es el resultado de varios inventarios, cada uno con distinto nivel de falta de información y actualización. En este sentido es importante contar con un **único inventario**, completo y actualizado.

4. **Falta de Recursos**

La provisión de recursos, aspecto fundamental para cualquier iniciativa que se quiera llevar adelante, pero en temas asociados con un SGSI resulta fundamental, y es tan importante que el estándar lo describe directamente en el punto asociado a las "Responsabilidades de la Dirección". Esto es claramente así, si no contamos con los recursos necesarios, resultará muy difícil implantar el SGSI y luego llevar a cabo las actividades asociadas al mantenimiento y mejora del mismo. Es la Dirección la encargada de brindar

los recursos necesarios. Para lograr el interés de la Dirección las áreas involucradas en los proyectos de SGSI recurren a distintos métodos, entre los que se pueden encontrar: charlas, talleres, relevamientos de seguridad, auditorias, etc.

5. Ausencia de Documentación

Si bien el estándar específica un apartado exclusivo orientado a los requisitos de documentación es poco frecuente encontrar que la Institución haya documentado en principio lo mínimo requerido por el estándar y además lo requerido para el correcto desarrollo de las actividades de negocio. En este sentido, en las Instituciones que se encuentra mayor documentación es en aquellas que han tenido experiencias asociadas a la implementación de otros Sistemas de Gestión, como pueden ser de la Calidad o de cuidado del Medio Ambiente o también en aquellas que deben cumplir alguna regulación que exige la existencia de procedimientos operativos documentados.

6. Ausencia de Roles y Responsabilidades

Las personas que integran una Organización deben tener claro qué deben hacer para ayudar al logro de los objetivos de negocio establecidos. Esto parece ser algo muy fácil de lograr e identificar, pero en temas asociados a seguridad de la información es un aspecto difícil de encontrar con el mismo nivel de madurez que en otras posiciones. Muchas personas que trabajan en áreas de seguridad o sistemas no tienen claro que deben hacer para ayudar al logro de los objetivos de la Organización. Esto es una responsabilidad de la Dirección y el estándar lo identifica claramente en el requisito 5.2.2. Recursos Humanos es el área responsable de definir las descripciones de puesto en conjunto con los referentes de área que correspondan, pero es esta área la que debe documentar el puesto y describir claramente las responsabilidades en materia de seguridad tanto de este puesto como de cualquier otro puesto en la Organización. Esto último no se encuentra con frecuencia en las Organizaciones, sino que las personas entienden que la seguridad depende de un área específica o “de sistemas”, y no es frecuente que se identifique como una responsabilidad de todos los miembros de la Organización. En los casos en los cuales se encuentra un nivel de madurez

superior es en aquellas industrias con fuerte regulación al respecto, como puede ser la industria financiera.

7. **Resistencia al cambio**

   Las personas se resisten a los cambios, esto no es una novedad, y obviamente no está fuera de las dificultades que vamos a enfrentar al momento de implantar un Sistema de Gestión de la Seguridad de la Información. Para ello debemos identificar los **agentes del cambio** que servirán de facilitadores para convertir la Política de Seguridad definida en algo tangible y objetivos cumplibles y evidenciables. Frases como “esto se viene haciendo así”, “no somos un banco”, “ya sabíamos esto” y un centenar de frases más, no son más que ejemplos de resistencia al cambio. Es importante tener en cuenta que la resistencia al cambio se debe reducir desde la Dirección de la Organización, es más, podríamos definirla como una nueva "responsabilidad de la dirección", dado que es ésta la que tiene que marcar el camino, brindar los recursos y apoyar cada una de las iniciativas que permitan establecer el programa de seguridad que permita llevar a la realidad la Política de Seguridad de la Información.

3.1.10 SELECCIÓN DE LA PLATAFORMA DE CONTROL Y LOS OBJETIVOS DE CONTROL

La plataforma de control seleccionada para el diseño del SGSI será el marco de control COBIT 4.1. Debido a que el sistema que se va a desarrollar en esta tesis es un Plan de Mejora y se plantea un Sistema de Gestión de Seguridad de Información, este va a estar enfocado básicamente en aquellos procesos de TI cuyo enfoque esté relacionado con los tres “pilares” de la seguridad de la información, que son: la integridad, la confidencialidad y la disponibilidad. Para esto se tomará en cuenta aquellos procesos de TI en cuyo enfoque se muestren como primario o como secundario, por último, si es que así se considere adecuado, según el giro del negocio, los pilares de seguridad de la información. En otros casos, puede ser que los procesos de TI no tengan que ver con ninguno de los tres enfoques mencionados, pero se incluirán para poder cumplir con la parte de administración de riesgos.

Por esta razón, los procesos de TI que actuarán como la plataforma de control del SGSI, y que serán especificados en la declaración de aplicabilidad, son los siguientes:

- PO2. Definir la arquitectura de la información
- PO4. Definir los procesos, organización y relaciones de TI
- PO6. Comunicar las aspiraciones y la dirección de la gerencia.
- PO8. Administrar la calidad.
- PO9. Evaluar y administrar los riesgos de TI.
- AI2. Adquirir y mantener software aplicativo.
- AI3. Adquirir y mantener infraestructura tecnológica.
- AI4. Facilitar la operación y el uso.
- AI6. Administrar cambios.
- AI7. Instalar y acreditar soluciones y cambios.
- DS1. Definir y administrar los niveles de servicio.
- DS2. Administrar los servicios de terceros.
- DS4. Garantizar la continuidad del servicio.
- DS5. Garantizar la seguridad de los sistemas.
- DS7. Educar y Entrenar a los usuarios.
- DS9. Administrar la configuración.
- DS10. Administración de problemas.
- DS11. Administración de datos.
- DS12. Administración del ambiente físico.
- DS13. Administración de operaciones.
- ME2. Monitorear y evaluar el control interno.

3.2 PLAN DE CONTINUIDAD DE NEGOCIO

Es importante mencionar algunos de los enfoques más relevantes al tema de un PCN usados internacionalmente, y que guardan cierta estrecha relación y a su vez diferencias. “El BCP es una disciplina que prepara a la organización a poder continuar operando durante un desastre, a través de la implantación de un plan de continuidad. Un PCN es un documento que contiene procedimientos y lineamientos para ayudar a la recuperación y restablecimiento de procesos

interrumpidos y recursos al estado de operación normal, en un tiempo prudencial"

- **Disaster Recovery Planning (DRP):** Se enfoca en la recuperación de los servicios de TI y los recursos, dados un evento que ocasionara una interrupción mayor en su funcionamiento.

- **Business Resumption Planning (BRP):** Se centraliza en la reanudación de los procesos de negocio afectados por una falla en las aplicaciones de TI. Se enfoca en la utilización de procedimientos relacionados con el área de trabajo.

- **Continuity of Operations Planning (COOP):** Busca la recuperación de las funciones estratégicas de una organización que se desempeñe en sus instalaciones corporativas.

- **Contingency Planning (CP):** Se enfoca en la recuperación de los servicios y recursos de TI, después de un desastre de dimensiones mayores o de una interrupción menor. Especifica procedimientos y lineamientos para la recuperación, tanto en áreas de la empresa como en las alternas.
- **Emergency Response Planning:** Su objetivo es salvaguardar a los empleados, el público, el ambiente y los activos de la empresa. Últimamente se busca de inmediato llevar la situación de crisis a un estado de control.

Todos los enfoques tienen un denominador común, el cual es su alcance tan estrecho. Cada una de las ópticas de planeación se centra en la protección de aspectos específicos de la organización, ignorando otras áreas críticas. Para entender esta limitación, se requiere un enfoque de planeación integrado, que permita proteger todas las áreas críticas de la organización.

3.2.1 Fases

3.2.1.1 FASE I BUSINESS IMPACT ANALYSIS (BIA)

Esta fase BIA consiste en identificar aquellos procesos relacionados con apoyar la misión de la empresa, y analizar con muchos detalles los impactos en la gestión comercial del negocio, si esos procesos fuesen interrumpidos como resultados de un desastre.

El entregable consiste en un informe en el cual se identifican las áreas del negocio que son críticas para el alcance de la misión de la firma, así como la magnitud potencial del impacto operativo y financiero de una interrupción en el desempeño de la empresa, y los requerimientos de tiempo para la recuperación de una interrupción del negocio.

3.2.1.2 FASE II GESTIÓN DE RIESGO

Las actividades de la gestión del riesgo evalúan las amenazas de un desastre, pormenorizan las vulnerabilidades existentes, los potenciales impactos de un desastre, identifican e implementan los controles necesarios para prevenir o reducir los riesgos de un desastre y terminan identificando escenarios de amenazas para aquellos procesos considerados esenciales en el BIA.

El entregable de esta etapa es un informe de Riesgos y Controles. Este documento identifica las posibles amenazas potenciales de interrupciones del negocio y los respectivos riesgos. Este informe puntualiza las recomendaciones para hacer el control de los riesgos que pudiesen alterar el normal desempeño de los procesos esenciales del negocio.

3.2.1.3 FASE III DESARROLLO DE ESTRATEGIAS DE UN PCN

Aquí se evalúan los requerimientos y se identifican las opciones p ara la recuperación de procesos críticos y sus recursos, en el escenario en que fuesen interrumpidos por un desastre.

El entregable es un informe en donde se pormenoriza la identificación de opciones viables para la recuperación de recursos y servicios, dada la posibilidad de que fuesen impactados por una interrupción del negocio. Por cada escenario

de amenazas se elaboran estrategias que contemplen los escenarios de amenazas identificados.

3.2.1.4 FASE IV DESARROLLO DE PLAN DE REANUDACIÓN DE OPERACIONES

La fase IV desarrolla un plan para mantener la continuidad del desempeño del negocio, basado en las fases previas, específicamente en la "gestión del riesgo" y en el Business Impact Analysis, así como en los aspectos planeados en el desarrollo de la estrategia de un PCN.

El entregable es un informe que contiene procedimientos y lineamientos concretos para la recuperación y el restablecimiento de los recursos dañados, y los procesos cuyo desempeño se ha interrumpido.

3.2.1.5 FASE V ENSAYO PCN

En esta fase se efectúa el ensayo del plan, con miras a poder determinar su grado de precisión y actualización.

Aquí el entregable son simplemente los registros que deben llenarse para demostrar a terceros que se realizan los ensayos, así como las acciones correctivas que la empresa debe emprender para hacer el ajuste al Plan de Reanudación de Operaciones.

3.2.2 Plan de Normalización de Servicios luego de la contingencia

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas. Cada uno de estos contará con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera: la restauración del servicio usando los recursos de la Institución, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios de los Sistemas de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente

para no perjudicar el buen servicio, como pata no perjudicar la operatividad de la Institución.

A continuación las actividades consideradas para la normalización luego de una contingencia.

Actividad	Responsable
Evaluar condiciones del centro de cómputo principal. Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se está afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuánto tiempo, etc. Adicionalmente se deberá avanzar en las labores de preparación del Centro de Datos Alterno.	Equipo de Cómputo.
Priorización de actividades del Plan de Continuidad. Toda vez que el BCP es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de la institución. Es importante evaluar la dedicación del personal actividades que puedan no haberse afectado, para ver su asignamiento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.	Comité de contingencia
Proceso de compras Poner órdenes de compra de reemplazo de equipos, órdenes de servicio y/o reparación en la medida de que sea necesario.	Jefe de Cómputo
Cobro de Pólizas de Seguro aplicables a los daños presentados durante la contingencia En el evento de que ocurriera una contingencia, y si estuvieran asegurados los activos de la institución, la primera opción para recuperar las operaciones normales es recurrir al cobro de pólizas de seguro. Si bien es cierto, que este dinero será devuelto en un plazo inmediato, eventualmente servirá para la adquisición de toda la infraestructura necesaria para que el negocio pueda funcionar paulatinamente como antes. Es vital entonces que el plan contenga la información clave del	Equipo de Comunicación

Actividad	Responsable
seguro que se adquiera en la institución.	
Supervisar la instalación del hardware, líneas , teléfonos, etc.	Equipo de logística
Validad si las acometidas eléctricas están en condiciones adecuadas de funcionamiento	Jefe de Cómputo
Verificar las condiciones de seguridad física del centro de datos y autorizar el reingreso del personal	Jefe de Cómputo
Inspeccionar las condiciones de operatividad de los equipos de cómputo	Jefe de Cómputo
Preparar todos los respaldos de sistema operativos, aplicaciones, base de datos, redes.	Jefe de Cómputo
Iniciar la fase de recuperación de información desde los registros manuales de contingencia o en base a la información del servidor de replicación.	Jefe de Cómputo
Inspeccionar las condiciones de operatividad de las instalaciones. Si está apto para recibir al personal autorizar su reingreso.	Jefe de Cómputo
Inicio de prestación de servicios en modalidad de prueba	Jefe de Cómputo
Comunicación del fin de la contingencia.	Jefe de Cómputo
Mejoramiento continuo del Plan de Normalización de los servicios de la contingencia.	Jefe de Cómputo

Pasos para la reactivación del servicio del Centro de Datos.

Paso	Actividad
1	Líder de Cómputo decreta la salida de línea del Sistema desde el Sitio alterno.
2	Equipo de Comunicaciones ordena la Sucursal.
3	Líder de Cómputo coordina con el proveedor de Comunicaciones, hacia el enlace principal restaurado
4	Jefe de Cómputo comunica el cambio exitoso al enlace principal de red.
5	Jede de Cómputo saca respaldos de los sistemas y se traslada con ellos al Centro de Datos.
6	Jefe de Cómputo carga respaldos de los sistemas y hace pruebas preliminares.
7	Jefe de Cómputo define y hace pruebas con la replicación entre el Centro de Cómputo

Paso	Actividad
	Principal y el Alterno (No se cuenta)
8	Jefe de Cómputo verifica comunicaciones a través de enlace restaurado.
9	Jefe de Cómputo coordina la entrada progresiva a usuarios a los sistemas, si el avance es el esperado, decreta operación desde el Centro de Cómputo Principal.
10	Equipo de Comunicaciones comunica a los puntos que pasen a modo normal.

Capítulo IV: REQUERIMIENTOS DE TI E INVERSIÓN DE LA SOLUCIÓN

4.1 COSTO DE LA INVERSIÓN

Descripción	S/
Servicio de consultoría Auditoria TI	14 000.00
Servicio de Implementación SGSI	14 000.00
Servicio de Implementación PCN	16 000.00
Total en Nuevos Soles	**44 000.00**
INC. IGV	

Son cuarenta y cuatro mil con 00/100 nuevos soles peruanos.
El Costo del Proyecto esta dimensionado en base a:

Honorarios profesionales calculados en base a una tasa horaria estimada del Equipo de Trabajo especializado y considerando los plazos previstos para la ejecución del proyecto.

- El pago será 50% de inicial y 50% a la finalización de los servicios
- La propuesta esta expresada en Nuevos Soles e incluye IGV.

En el presente se describirán todos los materiales necesarios para realizar la implementación de cada uno de los subsistemas descritos anteriormente. Luego se obtendrá el presupuesto que se requiere respecto a un plan de contingencia.

Ítem	Descripción	Cant.	P. Unit.	Total
01	**Mano de Obra**			
	Cableado de puntos de Data	70	12.00	840.00
	Cableado de puntos de Voz	20	12.00	240.00
	Instalación de puntos eléctricos	70	12.00	840.00
	Certificación de Puntos UTP *****	90	5.50	495.00
	Instalación de canaletas	160	1.60	256.00
	Instalación de tuberías	70	1.60	112.00

Ítem	Descripción	Cant.	P. Unit.	Total
	Perforaciones y Resanes Gbl	1	190.00	190.00
	Instalación de Cajas de pase	20	2.00	40.00
	Instalación de Tablero Eléctrico	1	36.00	36.00
	Rotulación y entregables Gbl	1	150.00	150.00
02	**Materiales**			
	Cable UTP Cat 5E DIXON x Cja	16	83.00	1,328.00
	Jack RJ45 Cat. 5E DIXON	90	1.25	112.50
	Face Plate doble DIXON	70	0.61	42.70
	Tapas ciegas para face plate DIXON	50	0.30	15.00
	Patch Panel 24 puertos DIXON	4	28.50	114.00
	Ordenadores Horizontales DIXON	2	8.50	17.00
	Patch cord de 5 Feet DIXON	70	1.03	72.10
	Cable 12 AWG THW Color rojo negro y amarillo x Rollo	15	43.00	645.00
	Tomacorrientes Leviton con puesta a tierra color naranja	71	5.43	385.53
	Cajas de montaje de 2" x 4" DIXON	140	1.03	144.20
	Canaleta de pared DXN 40x40 para data	48	4.40	211.20
	Canaleta de pared DXN 60x40 para data	12	6.61	79.32
	Canaleta de pared DXN de 25x40	25	4.10	102.50
	Canaleta de Piso DXN de 60mm	3	5.10	15.30
	Canaletas de pared de 40x40 para eléctrico	84	4.45	373.80
	Accesorios para Canaletas para data	50	1.35	67.50
	Accesorios para canaleta para eléctrico	50	0.80	40.00
	Tablero Eléctrico Con 10 llaves	1	55.00	55.00
	Transformado de aislamiento de 5 KV	1	72.00	72.00
	Tubos de 3/4 SAP para data	35	1.55	54.25
	Tubos de 1" SAP para eléctrico	35	2.20	77.00

Ítem	Descripción	Cant.	P. Unit.	Total
	Cajas de pase de 4x4 Data	12	1.53	18.36
	Cajas de pase de 4x4 para eléctrico	12	1.53	18.36
	Curvos de 3/4 para data	12	0.35	4.20
	Curvos de 1 para eléctrico	12	0.51	6.12
	HP 1910-24G Switch - Conmutador - Gestionado - 24 x 10/100/1000 + 4 x SFP - montaje en rack	1	335.00	335.00
	HP 1410-24G Switch - Conmutador - sin gestionar - 24 x 10/100/1000 + 2 x SFP compartido-sobremesa, montaje en rack, montaje en pared	1	250.00	250.00
			Sub Total	$7,854.94
			IGV	$1,413.89
			Total	$9,268.83

CONCLUSIONES

a. A través de su enfoque y marco metodológico de MAIGTI permitió dirigir de mejor manera las actividades de cada una de las fases de la auditoría facilitando con ello el análisis y evaluación del centro de datos, concluyéndose que tiene una seguridad insipiente, de baja aplicación de las normas técnicas y buenas prácticas, adolece de un SGSI.

   Uno de los factores de éxito en la realización de la Auditoria de Sistemas es el apoyo total y compromiso de la Gerencia, así como de los auditados al grupo auditor, de esta manera los auditores obtendrá la información necesaria para encontrar sus debilidades y así dar las mejores recomendaciones al auditado. De la misma manera, el auditado cumplirá y buscará el beneficio de la organización a través de las recomendaciones emitidas por el grupo auditor.

b. Continuamente se permite el ingreso al edificio a personas ajenas a las labores de la organización. Ej.: Personas que vienen a realizar gestiones de otras organizaciones que se encuentren en el mismo edificio y transitan por pisos que no son los correctos. El personal de recepción entrega un ticket de visitante y no pregunta a quien va a visitar la persona a la cual le entrega el ticket. Las puertas de acceso al centro de cómputo no tiene dispositivo para colocar clave y no se lleva un registro de quienes ingresan o salen del centro de cómputo, así como la hora en que se produjo la entrada o salida.

c. Están realizando procedimientos de control, están en camino de mejora alineados a buenas prácticas y lineamientos internacionales, Así mismo el Plan de Continuidad del Negocio es una manera de controlar el destino de la empresa. Básicamente tener un PCN significa en la organización que se han identificado los procesos esenciales, se han determinado los tiempos de recuperación máximos tolerables, bajo los cuales estos procesos pueden estar paralizados sin colapsar la empresa desde las perspectivas operacional y financiera.

d. Las normas de control interno se cumplen en un 50% por cambio de personal,

puesto que los encargados del área de cómputo, se retiraron borrando toda la información. Revisar el procedimiento de contratación de servicios con terceros que afecten servicios de TI en que se considere un análisis de riesgo previo por cambios de proveedores o cambios en el alcance del servicio.

Poner mayor énfasis en el Control de Cambios en los Sistemas, para clasificarlos debidamente de acuerdo a su urgencia y prioridad.

Necesariamente debe asignarse un responsable para administrar las fuentes en el ambiente de desarrollo, que sea quién libere los objetos mediante solicitudes aprobadas y sustentadas técnicamente.

e. Los escenarios de contingencia que cubre el Plan de Continuidad de Negocio son insuficientes para cubrir las operaciones de negocio ante catástrofes: incendio del edificio de la institución, terremotos, etc., se basan en un Plan de contingencia realizado para el Ministerio de Educación, que no se adecua al 100% con la institución.

f. El plan de mejora basado en el modelo ISO 27001:2005 y buenas prácticas COBIT requiere una participación completa a nivel estratégico. Su papel tiene que ser protagónico en la implantación del modelo.

   El auditor debe tener conocimiento claro sobre el entorno auditable, ya que, de esta manera explora más profundamente el proceso, y puede obtener resultados más objetivos respecto a la evaluación.

   De implantarse un Sistema de Gestión de Seguridad de la Información y la instalación de un ambiente de prueba, estos impactarán significativamente sobre la calidad de los sistemas de información.

RECOMENDACIONES

Se recomienda a todas las demás empresas o instituciones de los distintos rubros a contar con un Plan de Seguridad de la Información y/o un Sistema de Gestión de Seguridad de la Información que sería lo más indicado, ya que es importante que la información que manejan y que mueve su negocio se encuentre debidamente protegida, para evitar pérdidas de ventaja competitiva y, en el peor de los casos, el paro de la empresa. La información, en la actualidad, es lo único que mueve a la mayoría de las empresas. Si pasa un desastre y se pierde el edificio de la compañía se puede recuperar (lo más probable es que esté asegurado). Si asaltan a una empresa se puede recuperar una parte o todo el dinero, según el seguro con el que se cuente, pero si se pierde la información de la compañía simplemente la empresa deja de operar.

Una buena práctica en las organizaciones para las áreas de TI, en este caso Área de Cómputo es realizar periódicamente evaluaciones de riesgos con el objeto de minimizar los mismos y priorizar aquellos catalogados como riesgos altos. Así como también considerar evaluaciones periódicas de auditoría de sistemas que permitan identificar procesos a mejorar.

En la planificación de la Auditoría de Sistemas es necesario identificar correctamente los elementos que intervienen de modo que se tenga una visión global y concreta de los objetivos de la evaluación del proceso de auditoría.

Completar el inventario de activos asociados a la Tecnología de Información, realizar un análisis de los riesgos a los cuales cada uno de éstos se encuentra expuesto y asignar una clasificación de los mismos en función de la exposición de los riesgos.

REFERENCIAS BIBLIOGRÁFICAS

- Bertolín, J. A. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* Madrid: Learning Paraninfo, S.A.
- *Contraloría General de la República*. (s.f.). Recuperado el 2 de Abril de 2012, de https://apps.contraloria.gob.pe/dv/index.htm
- Hernández, R; Hernández, C. y P. Batista. (1997). *Metodología de la Investigación.* México: McGraw-Hill.
- Institute, I. G. (2007). *IT Governance Institute*. Recuperado el 10 de 01 de 2012, de Cobit 4.1: www.itgi.org
- *ITIL-Gestión de Servicios TI*. (s.f.). Recuperado el 10 de 10 de 2011, de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php
- Lopez, R. V. (1970). *Diseño Experimental no Parametrico.* Mexico: S. Trillas.
- Paredes, E. A. (2011). *Metodología para la auditoría integral de la gestión de las tecnologías de la información* (Vol. 1). Lima, Perú: Universidad Privada Norbert Wiener S.A - Fondo Editorial.
- Razo, C. M. (2002). *Auditoría en Sistemas Computacionales.*México: Pearson Education; 1st. edition.
- *Real Academia Española*. (s.f.). Recuperado el 4 de 1 de 2012, de http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=informaci%F3n
- *Real Académia Española*. (s.f.). Recuperado el 5 de Enero de 2012, de http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=contraloria
- Urbina Mancilla, R. (03 de 11 de 2006). Resolución de Contraloría General Nº 320-2006-CG. Lima, Perú.

ANEXOS

Anexo 1: Relación del Personal Entrevistado

Nombre	Cargo	Área	Fecha
Blanca Mostacero M.	Jefa de Cómputo	Cómputo	21-01-13
Edgardo Zegarra	Practicante de Sistemas	Cómputo	21-01-13

Anexo 2: Tabulación de Encuesta Usuarios Claves

I. SOBRE LOS SISTEMAS DE INFORMACIÓN		**Resultado %**
La información proporcionada por el Sistema es:	Oportuna	
	Correcta	
	Consistente	
	Confiable	
Al guardar información, realizar cálculos y realizar búsquedas y consulta, el sistema es:	Lento	
	Rápido	
	Normal en Velocidad	
Al utilizar el sistemas éste es:	Fácil de Usar	
	Complicado de Usar	
La búsqueda de información en el sistema es:	Flexible	
	Limitada	
A través de qué medios canaliza requerimientos de sistemas	Por teléfono	
	A través de un formato	
	Personalmente	
	Por correo electrónico	
	A través del jefe del departamento/área	

I. SOBRE LOS SISTEMAS DE INFORMACIÓN		Resultado %
	No hace requerimientos	
	Otros	
Tiene requerimientos que no haya solicitado	Si	
	No	
Utiliza todas la opciones del sistema	Si	
	No	

II. SOBRE EL DESARROLLO DE SISTEMAS Y HERRAMIENTAS		Resultado %
Durante el desarrollo Ud. participa en:	Solicitud de Requerimientos	
	Análisis y Diseño	
	Desarrollo	
	Pruebas	
	Implantación	
Ha recibido una buena capacitación en el uso del sistema	Si	
	No	

III. SOBRE EL SOPORTE DE SISTEMAS		Resultado %
Las caídas (fallas) del sistema son:	Frecuentes	
	Varias veces	
	Pocas veces	
	Nunca	
Siempre que hay estas caídas Ud.	Reporta e informa a Sistemas	
	Reinicia la computadora	
Ante requerimientos urgentes el soporte de sistemas es (helpdesk):	Oportuno	
	Poco oportuno	
	Inoportuno	
IV. ASPECTOS DE SEGURIDAD		**Resultado %**
Se le ha borrado información del disco duro	Si	
	No	
Sabe dónde guardar su información	Si	
	No	
Ha notado presencia de virus	Si	
	No	

III. SOBRE EL SOPORTE DE SISTEMAS		Resultado %
El área de sistemas le informa sobre nuevos virus	Si	
	No	
Comparte su password	Si	
	No	
Ha dado su password en caso de:	Vacaciones	
	Licencia	
	Enfermedad	
	Comisión	
	Nunca	
Ha recibido orientación en:	Niveles de Acceso a la información	
	Creación de claves de acceso	
	Cambio de claves periódicos	
	Copia de respaldo de documentos (word, excel, etc.)	
	Uso apropiado del Internet	
	Uso del Intranet	
	Que hacer en casos de fallas del Sistema	
	Confidencialidad de Información	

III. SOBRE EL SOPORTE DE SISTEMAS		Resultado %
	Buen uso de los recursos de cómputo	
Usa protector de pantalla con password	Si	
	No	
Deja la PC encendida al finalizar el día	Si	
	No	