UNIVERSIDAD ISRAEL

AUDITORIA INFORMATICA

INFORME FINAL

OSWALDO DURAN CRIOLO
06/07/2012

PLANEACION DE LA AUDITORIA DE SISTEMAS INFORMATICOS

INSTITUCION COORDINACION ZONAL 6 MIES

PERIODO AUDITADO : DEL 1 DE ENERO AL 31 DE DICIEMBRE DE 2012.

DIRECCION : BORRERO 4-24 Y CALLE LARGA

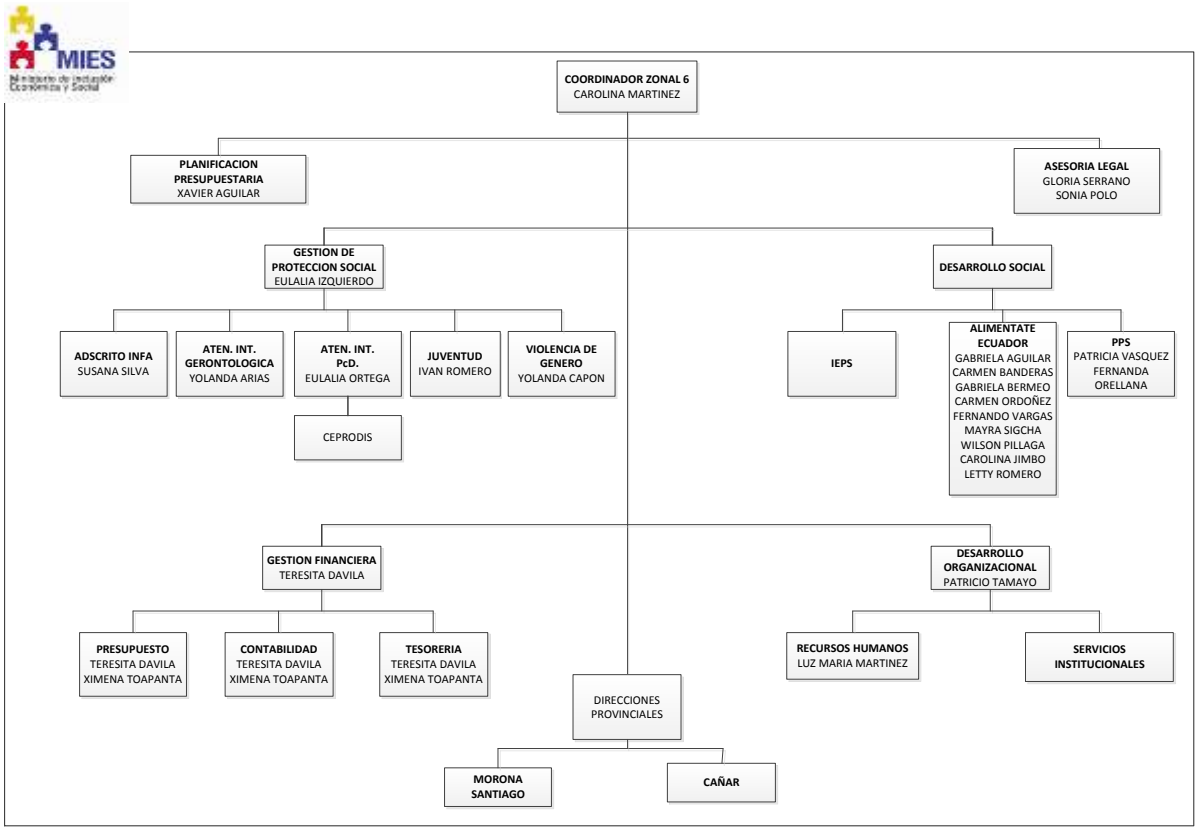
TELEFONO : 2837728

CUENCA ECUADOR

INICIO DE LA AUDITORIA 20 DE MAYO 2012

AUDITOR OSWALDO DURAN

ORGANIGRAMA COORDINACIÓN ZONAL 6 MIES



PERSONAL ENTREVISTADO:

Xavier Galarza - **Planificación**
Patricio Tamayo **– Desarrollo Organizacional**
Teresita Dávila **– Gestión Financiera**

INFORME FINAL

Etapas de la Metodología

1. Definición de Alcance y Objetivos

I. Antecedentes

La presente auditoria se realizara en las Oficinas de la Coordinación zonal 6.

El Ministerio de Inclusión Económica y Social (MIES) promoverá y fomentará activamente la inclusión económica y social de la población, de tal forma que se asegure el logro de una adecuada calidad de vida para todos los ciudadanos y ciudadanas, mediante la eliminación de aquellas condiciones, mecanismos o procesos que restringen la libertad de participar en la vida económica, social y política de la comunidad y que permiten, facilitan o promueven que ciertos individuos o grupos de la sociedad sean despojados de la titularidad de sus derechos económicos y sociales, y apartados, rechazados o excluidos de las posibilidades de acceder y disfrutar de los beneficios y oportunidades que brinda el sistema de instituciones económicas y sociales.

Como Coordinación, coordinamos el cumplimiento de compromisos presidenciales en la Zona 6, participamos en eventos nacionales, en el Plan Nacional del Buen Vivir, en la formulación y coordinación de la ejecución de la agenda zonal de desarrollo, en la capacitación y asesoría, en la formulación de los Planes de Desarrollo y Ordenamiento Territorial (PDOT), en la conformación de veedurías provinciales para el Plan Nacional del Buen Vivir, en la Junta de Autoridades de la Zona 6, en la formación del núcleo estratégico o sede del Ejecutivo en la Zona 6.

OBJETIVOS

1) Ampliar las capacidades de su población objetivo mediante la generación o garantía de las oportunidades de acceder a los servicios sociales de educación, formación, capacitación, salud, nutrición, y otros aspectos básicos de la calidad de vida que influyen en la libertad fundamental del individuo para vivir mejor.
2) Promover la inclusión económica de su población objetivo mediante la generación o garantía de las oportunidades de poseer, acceder y utilizar los recursos económicos de la sociedad para consumir, producir o realizar intercambios, de tal forma que se garanticen las oportunidades de acceso a trabajo, ingreso y activos.
3) Garantizar el derecho de su población objetivo a la protección social y especial, de modo que no sufran grandes privaciones como consecuencia de cambios materiales que afectan negativamente sus vidas, mediante la regeneración sistemática de un nivel mínimo de

ingresos y la protección o restitución de sus derechos económicos y sociales, de tal forma que se garanticen las oportunidades para vivir con seguridad y satisfactoriamente.

4) Fomentar la ciudadanía, la organización y la cohesión social mediante la promoción o garantía de participación de los ciudadanos y ciudadanas como actores fundamentales de su propio desarrollo, el reconocimiento de su capacidad transformadora y de emprender acciones que les permitan acceder o recobrar la titularidad de los derechos económicos y sociales, y la ampliación de las oportunidades de la población para interrelacionarse.

II. Objetivo General

Revisar y Evaluar los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la Coordinación Zonal 6 (mi trabajo) que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para un adecuado servicio a la sociedad.

III. Objetivos Específicos

- Evaluar el diseño y prueba de los sistemas del área de Informática
- Determinar la veracidad de la información del área de Informática
- Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.
- Evaluar la forma como se administran los dispositivos de almacenamiento básico del área de Informática.
- Evaluar el control que se tiene sobre el mantenimiento y las fallas de las Pcs.
- Verificar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.
- Garantizar el continuo servicio al público.

2. Estudio Inicial, Organización

I. Organigrama

El organigrama del MIES está establecido bajo acuerdo ministerial, por lo tanto no supone ningún error, no puede estar sujeto a cambios de la auditoria. El organigrama está establecido para cada Coordinaciones zonales de todo el país

II. Departamentos

Las actividades realizadas en cada uno de los departamentos están a cargo de personal especializado en cada área de trabajo, con actividades específicas, obviamente uno de ellos es el coordinador de proceso, capaz de toma de desuniones.

III. Relaciones jerárquicas y funcionales

El equipo de trabajo dentro del proceso cumple las relaciones funcionales y Jerárquicas previstas por el organigrama, Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

IV. Flujos de información

Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales.

Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

V. Número de puestos de trabajo

Los nombres de los Puesto de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas, por lo que no se da el caso de que: bajo nombres diferentes se realicen funciones idénticas", lo cual indica la no existencia de funciones operativas redundantes, número de puestos de trabajo verdaderamente diferentes.

VI. Número de personas por puesto de trabajo

La adecuación del personal determina que el número de personas es adecuado en cada proceso.

3. Entorno Operacional

I. Situación geográfica de los sistemas

No se determina Centros de Proceso de Datos en la institución. Cada proceso está encargado de custodiar su propia información.

II. Arquitectura y configuración de Hardware y Software

Los equipos están conectados a un servidor que provee Internet y correos institucionales al personal de todos los procesos, este servicio lo hace CNT a nivel nacional, al igual que todas las instituciones públicas.

La configuración y accesos restringidos se lo maneja desde MIES Planta Central.

III. Inventario de Hardware y Software

Inventario existente:

CPU
Monitor
Impresoras
Scanner
Mouse
Teclado
Discos duros externos
Switch
Modem
Hub

Windows XP
Windows 7
Quipux
Esigef

IV. Comunicación y redes

40 equipos conectados a un punto central.

4. Determinación de recursos de la Auditoría Informática

I. Materiales

i. Software

Programas propios de la auditoría:

Software: ACD auditor

Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

ii. Hardware

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado.

Para lo cual habrá de convenir el, tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

Horarios destinados:

Lunes-Viernes 18:00 – 21:00

Sábado, Domingo

II. Humanos

i. El equipo de auditoria está conformado por:

Coordinador General

Como responsable de la auditoria es necesario que sea poseedor de una gran experiencia en la materia, la cual puede derivarse de su formación académica y/o profesional, así como de su trayectoria y orientación personal.

3 años de experiencia de trabajo en informática y en instituciones públicas.

Líder de proyecto

En su carácter de enlace entre el coordinador general, el personal destacado en la auditoria, la organización y entorno, el líder representa el eslabón clave para que los objetivos, programa y estrategias propuestas sean susceptibles de alcanzarse.

Asistente o analista de proyecto

Como personal de primera línea, es el responsable de atender directamente a todo el personal que, de una u otra manera, interviene en la auditoria, además de ser quien va a manejar directamente los papeles de trabajo que contienen los hallazgos, evidencias y observaciones necesarios para derivar los criterios y propuestas que consoliden la aplicación de la auditoria.

ii. Elaboración del Plan y de los programas de trabajo

Luego de coordinar las actividades y una vez asignados los recursos, el coordinador de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el Plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos

- En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios
- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.
- El Plan estructura las tareas a realizar por cada integrante del grupo.
- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

5. Actividades de la Auditoría Informática

I. Técnicas de trabajo

Análisis de la información recabada del auditado
- Análisis de la información propia
- Cruzamiento de las informaciones anteriores
- Entrevistas
- Simulación
- Muestreos

II. Herramientas

Cuestionario general inicial
- Cuestionario Checklist
- Estándares
- Monitores
- Simuladores (Generadores de datos)
- Paquetes de auditoría (Generadores de Programas)
- Matrices de riesgo
- Matrices de riesgo
- Matrices de riesgo

Técnicas aplicadas dentro de las oficinas de la Coordinación Zonal

CICLO DE SEGURIDAD

Segmentos:

1. **Seguridad de cumplimiento de normas y estándares.**

   Es de vitan importancia analizar este aspecto, cumplir las normas de IEEE, ayudará a garantizar la seguridad en los sistemas informáticos de la institución.

2. **Seguridad de Sistema Operativo.**

El Sistema operativo es normalmente solo una porción del total de software que corre en un sistema particular. Pero el Sistema Operativo controla el acceso a los recursos del sistema. La seguridad de los Sistemas Operativos es solo una pequeña parte del problema total de la seguridad en los sistemas de computación, pero éste viene incrementándose en gran medida. Hay muchas razones para que la seguridad de los Sistemas Operativos reciba especial atención hoy en día.

3. **Seguridad de Software.**

   Garantizar que el software que utiliza la institución no sufra ataques, utilizando software de seguridad actualizado, con licencias para evitar que Software mal intencionado infecte a los programas y archivos de la Institución.

4. **Seguridad de Comunicaciones.**

   Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

   - **Autenticación y autorización**: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
   - **Integridad**: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza un metodo de comparación (Hash).Los algoritmos comunes de comparacion son Message Digest(MD) y Secure Hash Algorithm (SHA).
   - **Confidencialidad**: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES),Triple DES(3DES) y Advanced Encryption Standard (AES).
   - **No repudio**, es decir un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

5. **Seguridad de Base de Datos.**

   Incluye aspectos de:

   - Legales, sociales, éticos
   - Políticas de la empresa
   - Controles de tipo físico, acceso a as instalaciones
   - Identificación de usuarios
   - Controles del Sistema Operativo

- Tipos de usuarios:

6. **Seguridad de Proceso.**

En las entidades de tipo industrial, temas de diseño de productos, fórmulas de calidad, formas de control de calidad, saldos contables, inversiones de la organización, situaciones patrimoniales de su organización, sueldos y honorarios, premios al personal, etc. deberían ser revestidos de cierta confidencialidad también.

7. **Seguridad de Aplicaciones.**

Las aplicaciones es una de las capas más importantes en el ambiente de la tecnología de la información pero desafortunadamente muy ignorada desde la perspectiva de la seguridad. Me refiero, sobre todo, a las aplicaciones transaccionales donde realmente se hace el proceso y que residen en el back-end de la infraestructura (Legacy, Cliente Servidor, Distribuidas, Orientadas a Objetos, ERP´s, CRM´s etc.) y no a las que hoy día en el mercado se les pone mayor atención que son las basadas en Web.

8. **Seguridad Física.**

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no.
Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"(1). Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Fase 0: Causas de realización de una Auditoría de Seguridad

Con el avance acelerado, los sistemas informáticos que utilizan las empresas son cada vez más complejos, más ricos en funcionalidades y por tanto más difíciles de controlar, por lo tanto las instituciones nos resulta conveniente optar por realizar una auditoría de seguridad de los mismos para conocer exactamente cuáles son los fallos de nuestro sistema y evitar consecuencias indeseables, bien utilizando un software diseñado para ello bien recurriendo a servicios externos que las lleven a cabo.

Estas auditorías consisten en analizar el nivel de seguridad de nuestro sistema informático utilizando todo tipo de herramientas y técnicas para averiguar cuáles son los problemas a los que nos podemos enfrentar, presentarlos en un informe y proponer las medidas que sería necesario aplicar para solucionarlos.

Fase 1: Estrategia y logística del ciclo de Seguridad

Constituye la FASE 1 del ciclo de seguridad y se desarrolla en las actividades 1, 2 y 3:

Fase 1. *Estrategia y logística del ciclo de seguridad*

1. Designación del equipo auditor.
2. Asignación de interlocutores, validadores y decisores del cliente
3. Cumplimentación de un formulario general por parte del cliente, para la realización del estudio inicial

Los planes del equipo auditor se desarrolla de la siguiente manera:

1. Eligiendo el responsable de la auditoría su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a especialidad, pero compacto.

2. Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas, etc.

3. Mediante un estudio inicial, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su cumplimentación.

Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar la "tarea de campo", la operativa auditora del Ciclo de Seguridad.

4. Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.

La realización de entrevistas adecuadas constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado. Si esta no se produce, el responsable lo hará saber al cliente.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.

La entrevista concreta suele abarcar Subsecciones de una misma Sección tal vez una sección completa. Comenzada la entrevista, el auditor o auditores formularán preguntas al/los entrevistado/s. Debe identificarse quien ha dicho qué, si son más de una las personas entrevistadas.

Los Checklist's son útiles y en muchos casos imprescindibles. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede al levantamiento de la información correspondiente.

Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los Sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y volver a verificar los resultados de las pruebas auditoras.

La evaluación de los Checklists, las pruebas realizadas, la información facilitada por el cliente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoría, que se materializarán en el informe final.

A continuación, un ejemplo de auditoría de la Sección de Control de Accesos del Segmento de Seguridad Física:

Vamos a dividir a la Sección de Control de Accesos en cuatro Subsecciones:

1. Autorizaciones
2. Controles Automáticos
3. Vigilancia
4. Registros

En los siguientes Checklists, las respuestas se calificarán de 1 a 5, siendo1 la más deficiente y 5 la máxima puntuación.

Fase 2: Cálculos y Resultados del Ciclo de Seguridad

Cálculos y resultados del ciclo de seguridad

1. Cálculo y ponderación de Secciones y Segmentos. Las Subsecciones no se ponderan, solo se calculan.

2. Identificación de materias mejorables.
3. Priorización de mejoras.

En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoría de Seguridad.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Solo faltaría calcular el porcentaje de bondad de cada área; éste se obtiene calculando el sumatorio de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes.

Una vez realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:

- Autorizaciones 80%
- Controles Automáticos 70%
- Vigilancia 70%
- Registros 30%
- Promedio de Control de Accesos 62,5%

Cabe recordar, que dentro del Segmento de Seguridad Física, la Sección de Control de Accesos tiene un peso final de 4.

Prosiguiendo con el ejemplo, se procedió a la evaluación de las otras cuatro Secciones, obteniéndose los siguientes resultados:

Fase3: Operativa del ciclo de seguridad

Una vez asignados los pesos finales a todos los Segmentos y Secciones, se comienza la Fase 3, que implica las siguientes actividades:

1. Preparación y confirmación de entrevistas.

2. Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma. Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma

Fase4: Cálculos y Resultados del ciclo de Seguridad

1. Cálculo y ponderación de Secciones y Segmentos. Las Subsecciones no se ponderan, solo se calculan.
2. Identificación de materias mejorables.
3. Priorización de mejoras.

En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoría de Seguridad. El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Solo faltaría calcular el porcentaje de bondad de cada área; éste se obtiene calculando el sumatorio de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes. Una vez realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:
Autorizaciones 80%
Controles Automáticos 70%
Vigilancia 70%
Registros 30%

Fase5: Confección del Informe del ciclo de Seguridad

1. Preparación de borrador de informe y Recomendaciones.
2. Discusión del borrador con el cliente.
3. Entrega del Informe y Carta de Introducción.

CONCLUSIONES

CICLO DE SEGURIDAD

El ciclo de seguridad identifica posibles amenazas de las empresas, instituciones. La identificación de las amenazas permitirá la visualización de los puntos débiles que se podrán explotar.

Por lo tanto, la seguridad de la información debe ser garantizada en una forma integral y completa de ahí que resulte de mucha utilidad conocer con un poco más de detalle las medidas de seguridad que permiten movernos desde el análisis de riesgos hasta la administración de la seguridad.

Las medidas de seguridad son acciones orientadas hacia la eliminación de vulnerabilidades teniendo en mira evitar que una amenaza se vuelva realidad. Estas medidas son el paso inicial para el aumento de la seguridad de la información en un ambiente de tecnología de información, en empresas donde se maneja volúmenes de información, de no hacerlo lleva a la perdida.

CONCLUSIONES

La coordinación cuenta con sistemas de hardware y software que no dan problemas a la hora de cumplir con las actividades asignadas a cada funcionario.

Asimismo la distribución de personal es equitativa para las funciones que deben desempeñar.

No hay mucho trabajo para gente de tecnología, si para gente de ofimática.

RECOMENDACIONES

Se debe indicar que no cuenta con respaldos de ninguna información, en caso de posibles eventualidades todos los archivos se perderían. Por lo que se recomienda que se tome medidas urgentes para proteger los archivos.