ESCUELA SUPERIOR POLITECNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

I PROMOCION

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA"

PARTICIPANTES:
Lsi. Félix León Medrano
Ing. Mónica Mata Zavala
Ing. Sofía Mendoza Villacreses

2006

Índice

TEMA:

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA EL HONORABLE CONSEJO PROVINCIAL DEL GUAYAS"

INTRODUCCIÓN

Desde la década de los 70 los sistemas de información, las nuevas tecnologías y la automatización en general han formado parte del desarrollo y la evolución de las empresas, en un principio se diseñaron aquellos sistemas y aplicaciones orientadas al mundo del negocio, parecía obvio, sistematizando los procesos de las empresas se lograría un avance importante que mejoraba la productividad, competitividad y desempeño.

Los efectos de la informática y las telecomunicaciones y, en general lo que hoy en este mundo globalizado se conoce como las nuevas tecnologías, han constituido factores importantes para el desarrollo de las ciencias y la ingeniería en su conjunto.

Los avances tecnológicos han permitido el desarrollo de un sin número de industrias, y no sólo con equipos de la más alta tecnología que coadyuvan al mejoramiento y la productividad en la prestación de servicios, sino que también han focalizado sus esfuerzos para construir verdaderos sistemas de información capaces del manejo y almacenamiento de gran cantidad de datos, logrando sistemas complejos para la toma de decisiones.

Con este avanzar tecnológico y el mundo globalizado de hoy, en el cual se integran todo lo referente a recursos de información como hardware, aplicaciones, sistemas, almacenamiento y recurso humano; no podemos obviar un tema muy importante y que actualmente es de preocupación general para todas las empresas e instituciones públicas y privadas; nos referimos a la SEGURIDAD DE LA INFORMACIÓN.

ENUNCIADO DEL PROBLEMA

Antecedentes:

Los continuos avances tecnológicos como:

- Desarrollo del Internet y nuevas tecnologías asociadas al mismo.
- Incremento en el uso del correo electrónico.
- Incremento de usuarios de Internet en todo el mundo.
- Crecimiento del Comercio Electrónico sobre todo en los últimos años.
- Crecimiento de la industria del Software y Hardware.
- Y, desarrollo de las comunicaciones.

Han colocado a las organizaciones hoy en día frente a muchas necesidades como por ejemplo:

- Adquisición de nuevos productos y servicios informáticos
- Utilización del Internet como elemento que aporta para la gestión empresarial
- Necesidad creciente por brindar servicios a tiempo completo.
- Necesidad de obtener y brindar información en tiempo real
- Necesidad de integración de todos los procesos de las unidades de negocio.
- Uso de mejores tecnologías que coadyuven al manejo de la información.
- Búsqueda del orden y control en los procesos organizacionales.
- Búsqueda de la calidad de atención y la eficiencia, en función de la productividad, la asignación correcta de los recursos y la eficiencia económica.
- Búsqueda de estándares y mejores prácticas tecnológicas.
- Implementación de mecanismos de comunicación.
- Necesidad de ejecutar procesos críticos con mayor rapidez sin afectar los costos.
- Automatización de sus procesos mediante sistema y aplicaciones.
- Utilización de mejores herramientas en cuanto a hardware y software y uso de las comunicaciones.
- Significativa expansión en el número de personas que utilizan los recursos informáticos en su trabajo diario.
- Gran diversidad en plataformas computarizadas, frecuentemente incluyen una mezcla de arquitecturas de hardware y diversidad de software y aplicaciones.
- Disponibilidad de la información a nivel de toda la Institución.

- Implementación de nuevas tecnologías que se encuentren acordes con el cumplimiento de las leyes y reglamentaciones del mercado.

Al momento que todos estos elementos aportan una gran ventaja en las organizaciones y su uso e implementación intervienen en las organizaciones para lograr sus objetivos de productividad, competitividad y mejor desempeño, no podemos olvidar la seguridad de la información, sobre todo porque los ejecutivos de cada empresa deben conocer que la información es el "activo más valioso de su organización" y se torna necesario mantener como objetivo constante la salvaguarda de dicho activo, administrando correctamente los riesgos e impactos del uso de tecnologías existentes y nuevas, estableciendo seguridades y controles que minimicen daños o pérdidas de información y sobre todo garantizar la operatividad y continuidad del entorno empresarial.

Por lo tanto uno de los objetivos de las Organizaciones en la actualidad debería enfocarse a establecer mecanismos que prevean la Seguridad de su Información, mediante SISTEMAS DE GESTIÓN DE SEGURIDAD INFORMÁTICA que coadyuve a mantener la integridad, disponibilidad y confiabilidad de la misma.

JUSTIFICACIÓN

Un SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA tiene como objetivos generales:

- Concienciar a los miembros de las Organizaciones de la importancia de establecer mecanismos de seguridad informática estableciendo compromisos que van desde la más alta gerencia a todos y cada uno de los usuarios finales.
- Crear una cultura tecnológica y organizacional de evaluación de riesgos e impactos y administración de los mismos.
- Minimizar los riesgos en cuanto a pérdida de integridad, disponibilidad y confiabilidad de la información.
- Crear consideraciones de importancia con respecto a la seguridad de los sistemas y aplicaciones y de todo el entorno tecnológico.

- Analizar, diseñar y establecer mecanismos que permitan mantener la seguridad de las operaciones y la continuidad del negocio.

Por lo tanto su diseño e implementación tiende a minimizar la siguiente problemática en las Organizaciones:

- Desconocimiento, poco compromiso y apoyo de los más altos niveles gerenciales con temas relacionados a seguridad.
- Desconocimiento de responsables de tecnologías y usuarios finales de la importancia de la seguridad de la información.
- Pérdida de integridad, disponibilidad y confidencialidad de la información.
- Desconocimiento de procesos y mecanismos para proteger y salvaguardar la información.
- Riesgos e impactos por la utilización de nueva tecnología.
- Riesgos por ausencia o mal diseño de controles.
- Pérdida de la continuidad operacional.

La información y los procesos, así como las redes, sistemas y aplicaciones son activos comerciales importantes. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener una ventaja competitiva, flujo de caja, rentabilidad, conformidad legal e imagen comercial.

Cada vez más, las organizaciones y sus sistemas y redes de información se enfrentan a amenazas que afectan su seguridad, incluyendo fraudes por medio de computadoras, espionaje, sabotaje, vandalismo, incendio o inundaciones. Las fuentes de daño como los virus de computadora, ataques de piratas y negación de servicio se han vuelto más comunes, más ambicioso y cada vez más sofisticados.

La dependencia en los sistemas y servicios de información significa que las organizaciones son más vulnerables a las amenazas de seguridad. Las interconexiones de redes públicas y privadas y el compartir los recursos de información incrementa la dificultad de lograr un control de acceso adecuado. La tendencia a distribuir la computación ha debilitado la efectividad del control central especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser respaldada por una gestión y procedimientos apropiados. La gestión de seguridad de la información necesita, como mínimo, la participación de todos los empleados en la Institución, también pueden requerir la participación de los proveedores, clientes y accionistas. Así como es necesario que todos los procedimientos de seguridad queden debidamente documentados, con responsabilidades claras y establecidas por medio de un SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA. (*).

ENFOQUE DEL PROYECTO

Con el deseo de ayudar a las organizaciones a obtener los mecanismos de seguridad adecuados y aprovechando el interés de las mismas en temas relacionados al análisis, diseño e implementación de Sistemas de Información de Seguridad Informática, hemos contactado con el responsable del área tecnológica del H. Consejo Provincial del Guayas, Ing. Carlos Moreno Torres, quien nos ha manifestado su preocupación por establecer procesos que garanticen la seguridad de la información. Por lo tanto el presente proyecto está destinado a elaborar el Diseño de un Sistema de Gestión de Seguridad Informática, con la finalidad de fomentar las bases para su futura implementación de acuerdo a los parámetros establecidos en el diseño del mismo.

MARCO TEÓRICO

Cuando hablamos de sistemas se torna importante mencionar el concepto de una serie de términos relacionados, como los que se describen a continuación:

Tecnología: Los equipos (Hardware), programas (Software) y productos relacionados que permiten la entrega y funcionamiento de los sistemas de información.

Sistemas: Conjunto de elementos integrados, interrelacionados e interdependientes que se relacionan entre sí para cumplir con un objetivo.

(*) Texto extraído de la Norma ISO 17799.

Sistemas de Información: Un sistema que está diseñado para capturar, transmitir, guardar, recuperar y presentar información usada en uno o varios procesos del negocio.

Proceso de Negocio: Un grupo relacionado de pasos a actividades que usa recursos de personal, información y otros recursos para crear valor para clientes internos o externos.

Controles: Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Tipos de controles:

Preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Correctivos: Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Correctivos: Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Riesgo: Todo lo que pueda contribuir al fracaso en la obtención de los objetivos de una compañía.

La información es un activo que como otros activos comerciales importantes, tienen valor para una organización y en consecuencia necesita ser protegido adecuadamente. La seguridad de la información, protege a la misma de un rango amplio de amenazas para poder asegurar la continuidad comercial, minimizar los riesgos, maximizar el retorno sobre las inversiones y oportunidades comerciales.

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o utilizando medios electrónicos, mostrada en películas o habladas en conversaciones. Cualquiera que sea la forma que tome la información, o el medio que se comparta o sea almacenada, siempre se deberán proteger apropiadamente.

La seguridad de la información se caracteriza aquí como la preservación de:

Confidencialidad: asegurar que esa información sea accesible sólo a aquellos autorizados para tener acceso.

Integridad: salvaguardar la exactitud e integridad de los métodos de información y procesamiento.

Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando se los requieran.

La seguridad de la información se logra implementando un conjunto de controles adecuados, que podrían ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Se necesita estos controles para asegurar que se cumplan los objetivos de seguridad específicos de la Organización.

ISO / IEC 17799

El Estándar Internacional ISO (Organización Internacional para la Estandarización) / IEC (Comité Electrotécnico Internacional) 17799 fue preparado por la Institución de Estándares Británicos (como BS 7799) y fue adoptado, mediante un "procedimiento rápido" especial, por el Comité Técnico ISO / IEC JTC1, Tecnología de la Información, en paralelo con la aprobación dada por los organismos nacionales de ISO e IEC.

En el campo de la tecnología de la información ISO e IEC han establecido un comité técnico conjunto ISO / IEC JTC1. Los anteproyectos de los Estándares Internacionales adoptados por el comité conjunto son circulados entre los organismos nacionales para

su votación. La publicación como Estándar Internacional requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

Sistema de Gestión:

Un Sistema de Gestión implementa los procesos que permiten que una empresa realice un servicio o producto de manera confiable y en conformidad con unas especificaciones internacionales

Gestión de Riesgo

Gestionar o administrar los riesgos debe permitir a las Instituciones identificar, medir, controlar, mitigar y monitorear sus exposiciones al riesgo de operación a los que se encuentran expuestos en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objetivo social, tamaño, naturaleza, complejidad y demás características propias.

El proceso de administración de Riesgo tiene las siguientes etapas:

- Establecer un marco general
- Identificación de los riesgos
- Análisis de riesgos
- Evaluar y priorizar los riesgos
- Tratamientos del riesgo

OBJETIVO GENERAL DEL PROYECTO

Evaluar el entorno actual de la seguridad de la información en el H. Consejo Provincial del Guayas, diseñando un Sistema de Gestión de la Seguridad Informática que permita garantizar la integridad, disponibilidad y confidencialidad de la Información

ASPECTOS METODOLÓGICOS

El presente proyecto está orientado a realizar un diseño de un SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA, es decir cubrir con las etapas de análisis y diseño de Sistema, dejando así sentadas las bases sólidas para su futura implementación.

El proyecto tiene como base a la norma de Seguridad Informática ISO (Organización Estándar para la Estandarización) e IEC (Comité Electrónico Internacional) 17799: 2000, con sus 10 dominios y 16 objetivos de control. Cabe mencionar que la ISO/IEC 17799:2000; tiene como objetivo proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de seguridad. La norma ISO 17799:2000, nace de una revisión de BS (British Standard) 7799 en el año 2000.

El proyecto se encuentra conformado por cinco partes que se detallan a continuación:

Capítulo I: En la cual definirá el entorno organizacional de la Institución; como parte de un entendimiento general y necesario sobre la razón de ser de la misma, su misión, visión, cadena de valor, objetivos estratégicos, marco general. Se describirá de igual forma la infraestructura tecnológica actual del H. Consejo Provincial; brindando una breve explicación de plataforma IT en cuanto a hardware, software, sistemas de información, bases de datos, recurso humano y comunicaciones.

Capítulo II: Iniciando la presente se detallará una explicación breve de la norma ISO 17799:2000, y las razones por las cuales se ha escogido como base o pilar del presente proyecto, en comparación con otra metodologías y estándar como lo es COBIT.

Luego se analizará la situación actual con respecto a la seguridad de la información del H. Consejo Provincial del Guayas; para tal efecto se ha utilizado una herramienta extraída de COBIT y denominada "Modelo de Madurez" el cual permitirá identificar la situación actual de la Institución con respecto a la seguridad de su entorno tecnológico, definiendo la situación esperada bajo los parámetros establecidos en cuanto a tiempo, recursos y visión de la alta Gerencia por lograr los objetivos de seguridad deseados en el presente año.

Como parte final a este capítulo se realizará un análisis de riesgo en base a los 10 dominios propuestos por la ISO/IEC 17799, para lo cual se utilizará un programa de auditoria que permitirá aquellos riesgos que afecten la integridad, confidencialidad y disponibilidad de la información, evaluando su impacto y probabilidad de ocurrencia;

lo que ayudará a determinar los aspectos más críticos y riesgosos de la Institución con respecto a la seguridad de la Información, los cuáles se convertirán en el alcance del diseño del SGSI (Sistema de Gestión de Seguridad Informática).

Capítulo III: Este capítulo presenta el diseño del SGSI propuesto, en el cual se define el alcance del mismo y luego se realiza una gestión de los riesgos, lo cual incluye una evaluación de los controles existentes y una revisión controles inexistentes y que son propuestos por la Norma ISO/IEC 17799:2000.

En la evaluación de los controles existentes, se comprobará si los mismos cumplen con su diseño e implementación para lo cuál se utilizarán métodos de auditoria y obtención de evidencia. Dicha evaluación permitirá probar la efectividad y eficacia de los controles, y en su defecto recomendar controles adicionales o compensatorios que mejoren el nivel de seguridad de la Organización.

Capítulo IV: El presente capítulo presentará una declaración de aplicabilidad, la cual consiste en presentar a la Institución si todos aquellos controles evaluados, rediseñados, controles inexistentes y las recomendaciones establecidas, son aplicables para la organización y así establecer las bases para su futura implementación.

Capítulo V: El capítulo presenta un conjunto de recomendaciones generales del proceso del Sistema de Gestión de Seguridad de Información, que fueron observadas durante el mismo y que en opinión conjunta de los realizadores del presente proyecto se considera de importancia mencionar para mejorar la seguridad informática de la Institución.

Se presentará así mismo, un plan de acción propuesto para que la Institución implemente el SGSI detallado en el presente documento. El plan de acción será definido por las actividades a realizarse por cada dominio crítico especificado en nuestro alcance del SGSI, y se especificarán los tiempos y personal propuesto para la ejecución de las actividades de mejora.

Como parte final se presentarán la conclusión general del SGSI, Sistema de Gestión de Seguridad Informática, para el H. Consejo Provincial del Guayas.

APLICACIÓN PRÁCTICA. IMPACTOS ESPERADOS (SOCIALES, ECONÓMICOS, CULTURALES, COMPETITIVOS).

El desarrollo de un SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA para el H. Consejo Provincial del Guayas, coadyuvará de forma significativa a minimizar los riesgos inherentes a los problemas de seguridad de la Institución.

El SGSI dará a conocer los lineamientos y parámetros de seguridad necesarios que deberán ser considerados para futura implementación y así colocar a la Institución en un nivel de seguridad adecuado y aceptable; la correcta administración y gestión de los riesgos tecnológicos permitirán a la Institución obtener ahorros en cuanto a tiempo, esfuerzos y recursos; de una manera organizada y planificada; lo cual constituyen parámetros para obtener una significativa ventaja competitiva frente a otras Instituciones del sector público que no han inicializado sus procesos de resguardo y seguridad de activos y de información.

Así mismo el presente proyecto tiene como objetivo coadyuvar con las Organizaciones para emprender un proceso de certificación basada en la norma internacional ISO 17799. Al finalizar la etapa de diseño y luego con la correcta decisión de implementación del SGSI propuesto, la Institución podrá emprender un proceso de certificación mediante la norma menciona.

INSTITUCIONES USUARIAS:

El presente proyecto está destinado para todas aquellas organizaciones preocupadas por la seguridad de la información.

En base a que el desarrollo del SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA se realizará para una Institución Pública, el proyecto puede ser de gran utilidad para fijar las directrices y el diseño de un sistema de seguridad de la información en base a parámetros de entorno económico, social y requerimientos y exigencias legales de las Instituciones Públicas a nivel Nacional o toda aquella Organización que necesitase los lineamientos necesarios para empezar un proceso de certificación bajo la norma ISO 17799.

CAPÍTULO I

MARCO GENERAL DE LA ORGANIZACIÓN

INSTITUCIÓN: HONORABLE CONSEJO PROVINCIAL DEL GUAYAS

El H. Consejo Provincial del Guayas, nace de acuerdo a la constitución de la república realizada en 1906; la cual establece lo siguiente: a) Nominación definitiva de la Institución Provincial, b) Determinación específica y amplia de atribuciones; c) Integración de los Consejos Provinciales, y d) Separación del Consejo Provincial de las Municipalidades.

Definitivamente luego de lo mencionado, teníamos Consejos Provinciales estructurados, pero no es hasta 1.945 cuando se constituyen de forma total la estructuración jurídica de los organismos seccionales; y más aún otorga a una ley especial la facultad de normar el funcionamiento de los Consejos Provinciales.

ENTORNO INSTITUCIONAL:

De acuerdo a datos históricos la Provincia del Guayas fue creada el 31 de Julio de 1824, de acuerdo a la Ley de División Territorial que dictó el Gral. Francisco de Paula Santander, y en virtud de la cual se creó el Estado de Quito, fraccionado en tres Departamentos: Ecuador -Quito-, Azuay y Guayaquil.
La iniciativa del Prefecto Provincial del Guayas, Econ. Nicolás Lapentti Carrión, dio inicio a un serio análisis histórico que determinó como fecha de nacimiento de la Provincia del Guayas, el 8 de Noviembre de

1820, día en se reunió el Colegio Electoral o el Congreso de la Provincia Libre de Guayaquil conformada por lo que hoy son los territorios de las provincias de Guayas, Los Ríos, El Oro, Manabí y Galápagos.
Se conformó el Colegio Electoral con 58 diputados, 16 correspondientes a Guayaquil y los restantes de Machala, Santa Elena, Montecristi, Jipijapa, Chone y la Isla Puná.

La reunión la hicieron en el lugar donde hoy se levanta el Palacio Municipal de Santiago de Guayaquil. En ese acto se eligió a Don José Joaquín de Olmedo y Maruri, como el primer Presidente de los territorios Libres de lo que hoy es el Ecuador. Fue Olmedo quien redactó lo que es la Primera Constitución Política del Ecuador, cuyo instrumento legal dio inicio a una República pequeña y Libre, dotada de una Constitución, sus propio Ejército y Marina, su Administración de Justicia, organizó la Hacienda Pública, dictó las primeras leyes, su bandera, su religión, los primeros impuestos; es el documento que sentó las bases del Constitucionalismo de lo que hoy es el Ecuador, documento que inspiró a la que posteriormente se aprobó en Riobamba. La Constitución de Guayaquil Independiente es el ejemplo pionero que sustenta nuestra nacionalidad.

LA PROVINCIA DEL GUAYAS.- Su nombre es tomado del más importante río de la costa ecuatoriana, el río Guayas, que sin lugar a dudas es el accidente hidrográfico más grande e importante del Pacífico Sur.

SITUACION Y LIMITES.- Está situada en el suroeste del Litoral: limita al Norte con las provincias de Manabí, Pichincha y Los Ríos. Al Sur con la provincia de El Oro. Al Este con las provincias de Los Ríos, Chimborazo, Cañar y Azuay. Y al Oeste con el Océano Pacífico.

CAPITAL.- Su capital es Guayaquil, Ciudad fundada en 1.537, por Francisco de Orellana. Está ubicada cerca de la desembocadura del río Guayas, es la ciudad más poblada y económicamente más activa del Ecuador.

POBLACION.- La Provincia del Guayas tiene una población de 3'256.763

habitantes, 1'626.077 hombres y 1'630.686 mujeres. Habitan en el área urbana 2'661.057 personas; 1'312.555 hombres y 1'348.502 mujeres. Mientras que en el área rural viven 595.706 personas, siendo 313.522 hombres y 282.184 mujeres.

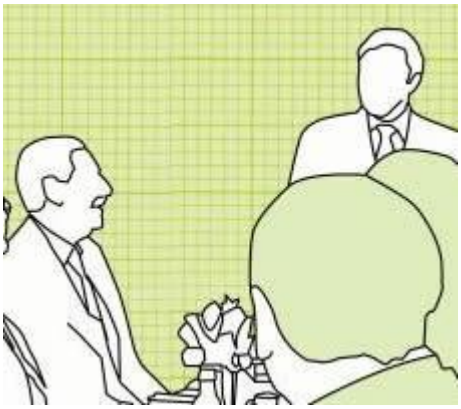
La población tiene un rápido crecimiento, especialmente la urbana, debido a las importantes corrientes migratorias internas, de distintas zonas del país, que le confieren un acentuado carácter heterogéneo.

Hay que destacar que desde la época de la colonia e inicios de la República se han establecido inmigrantes de diferentes países de Europa, Asia y Medio Oriente cuyo aporte al desarrollo de las actividades económicas, artísticas y culturales ha sido importantes.

DIVISION POLITICA.- La Provincia del Guayas tiene como su Capital a la ciudad de Guayaquil, conocida también como Perla del Pacífico y está dividida políticamente en 28 cantones, 50 parroquias urbanas y 35 parroquias rurales.

ESTRUCTURA

El H. Consejo Provincial en su estructura interna se compone principalmente de las siguientes comisiones:



- Municipalidades
- Obras Públicas y Vialidad
- Vivienda Popular
- Legislación y Redacción
- Educación Pública y Deportes
- Economía y Finanzas
- Límites
- Rellenos y Muros de Contención
- Peaje y Pontazgo
- Patios y Canteras
- Espectáculos
- Desarrollo Rural Integral

- Coordinación, Fomento, Turismo y Propaganda
- Cuestiones Sociales, Sanidad e Higiene
- Comisión Especial de Asuntos Peninsulares

ACTIVIDADES Y FUNCIONES

El H. Consejo Provincial del Guayas para determinar límites de autoridad y responsabilidad de los diferentes niveles, de acuerdo con una adecuada división de trabajo de las unidades administrativas que conforman la Corporación, establece su Reglamento Orgánico Funcional:

TITULO II DE LAS FUNCIONES

CAPITULO I
DEL NIVEL LEGISLATIVO

Art. 7.- El Consejo Provincial tiene las siguientes facultades:

- Aprobar las ordenanzas, reglamentos, acuerdos, resoluciones y otras normas legales que beneficien el desarrollo de la Corporación y de la provincia;

- Establecer las políticas y lineamientos básicos, que deben ser implantados en los diferentes niveles administrativos;

- Aprobar el presupuesto anual, cuya proforma será presentada por la Prefectura hasta el 20 de julio de cada año;

- Crear y/o reformar las tasas para los servicios públicos que se establecieren en la

provincia, de acuerdo con la respectiva Ley;

- Expropiar inmuebles por causa de utilidad pública o interés social de acuerdo con la Ley;

- Ejercer las atribuciones que le concede la Ley de Caminos en las vías que construya o mantenga;

- Informar al Congreso la conveniencia o inconveniencia de la creación de cantones y parroquias;

- Autorizar gastos de acuerdo con las normas legales correspondientes; Conceder licencia al Prefecto y Consejeros hasta un total de 60 días cada año; Nombrar y remover a los Directores o Jefes del más alto nivel y/o encargar dichas funciones por ausencia del titular.

- Fijar las remuneraciones, sueldos, salarios y demás beneficios sociales de los empleados y trabajadores de acuerdo con las normas legales vigentes;

- Conocer y dictaminar sobre las resoluciones que expidan las Municipalidades de su jurisdicción territorial para donar inmuebles de su propiedad, de conformidad con lo previsto en la Ley respectiva;

- Conceder licencia que pase de 60 días a los funcionarios de la Corporación; y Ejercer las demás atribuciones señaladas en la Constitución y demás Leyes.

CAPITULO II
DEL NIVEL EJECUTIVO

Art. 8.- El Nivel Ejecutivo está representado por el Prefecto Provincial, cuyas atribuciones son las siguientes:

- Presidir las sesiones del Consejo, con voto dirimente; someter a su resolución todas las cuestiones de interés provincial; y llevar a conocimiento de la

Corporación, las solicitudes de particulares u organizaciones que deben ser consideradas por ésta;

- Presentar a consideración y aprobación del Consejo un plan general de actividades para el período para el que fue elegido;
- Representar al Consejo Provincial, conjuntamente con el Procurador Síndico, en todos los asuntos judiciales y extrajudiciales de la institución; Suscribir en unión del Procurador Síndico, los contratos ya aprobados por el Consejo Provincial;
- Ordenar las adquisiciones y autorizar el pago de los servicios y obras de la Corporación, ciñéndose a las disposiciones legales y presupuestarias;
- Suscribir la correspondencia oficial, las actas de las sesiones del Consejo, así como las ordenanzas y resoluciones;
- Disponer la convocatoria a sesiones ordinarias y extraordinarias de la Corporación;
- Nombrar y remover, con acatamiento de la Ley de Servicio civil y Carrera Administrativa, a los empleados cuya designación no corresponda hacer al Consejo, así como contratar y remover a los trabajadores del Consejo sujetos al Código del trabajo y a roles, de acuerdo con la Ley;
- Vigilar que los empleados de la Corporación cumplan con su deber;
- Controlar permanentemente, la marcha de los aspectos financieros;
- Designar comisiones especiales para asuntos que deban ser resueltos por el Consejo y que no hubieren sido asignados a las comisiones; Resolver, administrativamente, todos los asuntos que no fueren de incumbencia del Consejo;
- Informar al Consejo, hasta el 31 de julio de cada año, acerca de las labores desarrolladas durante el año anterior, informe que lo hará extensivo al Ministro de Gobierno;
- Cumplir y hacer cumplir la Ley, las ordenanzas, acuerdos y resoluciones que dicte el Consejo Provincial;
- Aceptar, con autorización del Consejo, con juntamente con el Procurador Síndico las herencias, donaciones o legados que se hicieren a favor de la Corporación;
- Ordenar, de conformidad con la Ley, la baja de especies y de bienes;
- Ordenar los gastos, de acuerdo con las partidas presupuestarias y las

disponibilidades de caja, así como los gastos extraordinarios con cargo a la partida de imprevistos, hasta por la suma determinada en el presupuesto, con la obligación de dar cuenta al Consejo;

- Conceder licencia a los empleados, hasta por un total de sesenta días al año, con sueldo de acuerdo a la Ley;
- Fijar los salarios y emolumentos de los obreros del Consejo que no trabajen a sueldo fijo, con observancia a las disposiciones legales vigentes; y
- Ejercer las demás atribuciones que le concedan la Constitución Política del Estado, la ley de Régimen Provincial y demás normal legales.

Art. 9.- La Vicepresidencia está representada por el vicepresidente del Consejo cuyas funciones son:

- Subrogar al Prefecto Provincial en caso de ausencia temporal;
- Presidir comisiones especiales de trabajo;
- Participar en la formulación de planes, programas y proyectos del Honorable Consejo Provincial;
- Apoyar a la Prefectura en tareas relativas al establecimiento de lineamientos y políticas para la formulación de programas a corto, mediano y largo plazo;
- Coordinar los estudios y trabajos relacionados con los mecanismos interinstitucionales para el fortalecimiento de la Corporación;
- Asumir por delegación expresa, la Prefectura del Honorable Consejo Provincial; y
- Las demás funciones que le asigne el Prefecto Provincial.

Art.10.- La Presidencia Ocasional está representada por el Presidente Ocasional, cuyas funciones son:

- Subrogar al Vicepresidente del Consejo en caso de ausencia temporal;
- Presidir comisiones especiales de trabajo;
- Apoyar a la Prefectura y al Vicepresidente del Consejo en tareas relativas al establecimiento de lineamientos y políticas para la formulación de planes, programas y proyectos;
- Diseñar y proponer el establecimiento y operación de mecanismos de coordinación a nivel institucional; y

- Asumir por delegación expresa, la Prefectura del H. Consejo Provincial por falta de Prefecto y Vicepresidente.
- Las demás funciones que le asigne el prefecto Provincial.

MISIÓN

- Diseñar, ejecutar y evaluar el Plan Provincial de la Provincia del Guayas que permita mejorar la calidad y condiciones de vida de sus habitantes.

VISIÒN

- Lograr la ejecución del Gobierno de la Provincia del Guayas, descentralizado y autónomo, que lidere con efectividad y eficiencia el proceso de desarrollo humano e incorpore a su gestión la participación de los ciudadanos, atendiendo de forma efectiva las necesidades de la comunidad guayasense.

OBJETIVOS

1. Fortalecimiento institucional a través del conocimiento de la Visión y Misión.
2. Colaborar con las redes de información tecnológica.
3. Formular políticas para el desarrollo sustentable.
4. Atender en cuestiones de vialidad, salud y educación a la comunidad guayasense.
5. Formular políticas de comunicación para el desarrollo.
6. Elaborar propuestas de cambios del marco legal.
7. Formular políticas para transparentar la gestión pública.
8. Formular proyectos intra e interprovinciales en Coordinación con los demás organismos seccionales y municipales.
9. Promover las organizaciones de las comunidades para formular, ejecutar y evaluar los planes de desarrollo comunitario.

AMBIENTE REGULATORIO

Las leyes que rigen al H. Consejo Provincial del Guayas son:

- Constitución Política de la República del Ecuador
- Código del Trabajo del Ecuador
- Ley Especial de Descentralización
- Ley de Modernización del Estado y Privatizaciones
- Ley del Régimen Provincial
- Ley Orgánico de Servicio Civil y Carrera Administrativa
- LOAFIC (Ley Orgánica de Administración Financiera y Control)
- Reglamento a la ley de descentralización
- Ley Orgánica de Transparencia y Acceso a la Información Pública

CADENA DE VALOR DEL H. CONSEJO PROVINCIAL DEL GUAYAS

ESTRUCTURA ORGÁNICA

El H. Consejo Provincial del Guayas consta actualmente con la siguiente estructura orgánica detallada a continuación por Direcciones:

- Prefectura
- Auditoria Interna
- Dirección Financiera
- Dirección Administrativa
- Dirección de Recursos Humanos
- Dirección de Planificación
- Dirección de Obras Públicas
- Dirección de Concesiones
- Coordinación Ejecutiva
- Secretaría General
- Relaciones Públicas
- Dirección de Fiscalización
- Dirección de Turismo
- Vicepresidencia
- Presidencia Ocasional
- Sala de Comisiones (H. Consejeros Provinciales)
- Procuraduría Sindica
- Proyectos Especiales

Cada Dirección cuenta con Subdirecciones, Jefaturas y Secciones.

Para efectos de este trabajo no se ha incluido el orgánico funcional de la Institución, el cual se encuentra en proceso de aprobación.

El recurso humano dentro de la Institución se clasifica de acuerdo a los tipos de empleados detallados a continuación:

- Obreros Ocasionales
- Obreros de Planta
- Contratados
- Nombramiento
- Asesores

ESTRUCTURA ORGANIZACIONAL DEL ÁREA DE IT

El área de tecnología dentro de la Institución está a cargo de la Coordinación de Informática, dicha área forma parte de la Dirección Financiera a nivel de Subdirección.

La Coordinación de Informática tiene la siguiente estructura interna:

- Coordinador de Informática
- Jefatura de Redes y Comunicaciones
- Jefatura Técnica
- Jefatura de Desarrollo
- Jefatura de Producción
- Jefatura de Seguridades Informáticas.

ADMINISTRACIÓN Y PLANEACIÓN DE SI

- La Coordinación de Informática cuenta con un plan estratégico del año 2005, alineado con los intereses Institucionales y objetivos del negocio.
- Existe una política de seguridad cuya última actualización fue realizada en febrero del año en curso.
- Existen políticas y procedimientos establecidos de trabajos, entre los cuales podemos citar:
    - Procedimiento de cambio de claves
    - Procedimiento de creación, bloqueo y eliminación de usuarios de red.
    - Procedimiento de creación, bloqueo o eliminación de cuentas de Internet.
    - Procedimientos de atención a usuarios finales.
    - Procedimientos de mantenimiento de equipos informáticos.
    - Procedimientos de cambio de partes y piezas en equipos informáticos.
    - Procedimiento de compra de bienes de infraestructura tecnológica.
    - Procedimientos de respaldo.
    - Procedimientos de ejecución de garantías.
    - Procedimientos de pasos de programas de ambiente de desarrollo a producción.
    - Procedimientos de cambios en las aplicaciones.

- Procedimientos de creación, bloqueo y eliminación de cuentas de usuarios de base de datos.
- Procedimiento de monitoreo de base de datos, entre otros.

Existen políticas establecidas a nivel de la red como las que se mencionan a continuación:

- Política de escritorio
- Políticas de horarios de acceso a la red.
- Políticas para compartir recursos.
- Políticas de impresión.
- Políticas de respaldo y almacenamiento de información de usuarios finales.
- Políticas de uso de hardware.
- Políticas de usuarios de software.
- Políticas de niveles de usuario.
- Políticas de distribución de servicio.

INFRAESTRUCTURA TÉCNICA:

Hardware	Usuario Final	Equipos marca IBM, HP en un 80%, equipos clones en 20%. Características generales de los equipos: Procesador Pentium III a Pentium IV Memoria de 128 y 256 MB en promedio. Disco Duro de 40 GB Disquetera, CD ROM. Monitores de 15 pulgadas.
	Centro de Cómputo	2 servidores SUN SOLARIS (Desarrollo y Producción) 1 Servidor IBM (dominio) 1 Servidor DELL (Respaldo) Equipos de características menores que son utilizados para los siguientes servicios: Proxy, Antivirus, Drivers y Firewall.
	Equipos de comunicación	Switch Cisco capa 3 administrables (7) Switch Nortel Routeador Cisco utilizado para enlace de datos entre las dos dependencias de la Institución.

	Respaldo	Unidades de Cinta (SUN SOLARIS) SUN Storage (6 discos).
	Voz sobre IP	Multitech (2)
	Seguridad	Firewall Pix Firewall por software.
Software	Usuario final	Windows 2000 Profesional Office 2000 estándar Antivirus corporativo Norton Autocad (en áreas autorizadas) Internet Explorer Windows Media Player WinZip Acrobat 6.0 Service Pack. Runtime (Oracle) Developer 6i (PC´s de Desarrollo) Toad (PC´s de Desarrollo) Erwin (PC´s de Desarrollo)
	Centro de Cómputo	SUN SOLARIS Windows 2000 Windows 2003
	Mensajería	Nopopud (mensajería interna) Outlook (en caso de usuarios con cuentas de correo).

Comunicaciones	Datos	Cableado categoría 5e. Aproximadamente 500 puntos de datos, de los cuales son utilizados 190 en el edificio central y 60 en dependencias de galpones (Atarazana- Administración). Closet de Telecomunicaciones ubicado en el tercer piso del edificio central, para servicio a los pisos adyacentes.
	Voz	Existen aproximadamente 400 puntos de voz, de los cuales son utilizados actualmente 200. La utilización de voz sobre IP es usada para la comunicación entre las dos dependencias de la Institución.
	Video	Transmisión de video entre las oficinas centrales y las dependencias de atarazana, incluso transmisión de video por la red del edificio central.
	Enlace de datos	Enlace inalámbrico de 5.8 GHZ, con saltos de repetición en edificio "La Previsora" y "Porta". Marca de equipos utilizadas: TELETRONICS. Proveedor de servicio externo de enlace y mantenimiento del mismo. Enlace para comunicación interna entre dos edificios de la dependencia atarazana, con enlace inalámbrico de 2.4 GHZ.

Base de Datos	Servidor de Producción. Servidor de Desarrollo.	Oracle 9i Ambiente de desarrollo: Oracle Developer 6i.
Aplicaciones		Ruteo y seguimiento de trámite Contabilidad y Presupuesto. Coactiva Catastro Resoluciones Recaudaciones Seguros Síndico Planificación Obras Públicas Compras y ruteo Existencia Activos Fijos Talleres y repuestos Combustibles Auditoria Recursos Humanos Turismo Fiscalización Brigadas Médicas Prefectura Seguridad Unidad de concesiones Relaciones Públicas Sala de Comisiones Secretaría General.

INVENTARIO DE LAS APLICACIONES

Como se listó anteriormente existen un total de 29 aplicaciones desarrolladas para la Institución, a continuación se dará una breve descripción con respecto a las aplicaciones:

- Aplicaciones desarrolladas en sitio por personal externo, el H. Consejo Provincial del Guayas mantiene terciarizado su departamento de desarrollo con una empresa Consultora que ejecuta el desarrollo y mantenimiento a las aplicaciones.

- Actualmente existen aplicaciones en proceso de implementación y aplicaciones en mantenimiento.

- La principal aplicación que constituye una de las más completas y con nivel transaccional alto, corresponden a las aplicaciones desarrolladas para el área Financiera.

- El nivel de dependencia de la Institución con respecto a las aplicaciones es medio ya que el área de tecnología representa un soporte a la cadena de valor del negocio.

- Las aplicaciones forman parte del Sistema Automatizado para el Consejo Provincial (SAC), cuyo desarrollo fue realizado en herramientas de Oracle (Developer 6) y Base de Datos Oracle 9i.

DETALLE DE APLICACIONES

Aplicación	Base de Datos	Sistema Operativo	Interrelación con otras aplicaciones
Prefectura	Oracle 9i	SUN SOLARIS	Recursos Humanos Ruteo – Seguimiento Compra y ruteo

			Secretaría General Sala de Comisiones Sindico Relaciones Públicas
Ruteo y Seguimiento	Oracle 9i	SUN SOLARIS	Recursos Humanos Compras Proveeduría Existencia
Contabilidad y Presupuesto	Oracle 9i	SUN SOLARIS	Recursos Humanos Compras y ruteo Existencia Bodega de Proveeduría Sindicatura. Secretaría General
Catastro	Oracle 9i	SUN SOLARIS	Obras Públicas Planificación Recaudaciones Coactiva
Coactiva	Oracle 9i	SUN SOLARIS	Catastro Recaudaciones
Recaudaciones	Oracle 9i	SUN SOLARIS	Contabilidad y Presupuesto Resoluciones
Activos Fijos	Oracle 9i	SUN SOLARIS	Contabilidad y Presupuesto Existencia Hardware Compras y ruteo Recursos Humanos
Existencia	Oracle 9i	SUN SOLARIS	Compras y ruteo Mantenimiento y talleres Activos fijos

			Recursos Humanos
Resoluciones	Oracle 9i	SUN SOLARIS	Aplicaciones menores como Vallas publicitarias, títulos de crédito. Recaudaciones.
Compras y ruteo	Oracle 9i	SUN SOLARIS	Bodega de Proveeduría Existencia Mantenimiento y talleres Contabilidad y Presupuesto. Ruteo y seguimiento de trámite.
Mantenimiento y talleres	Oracle 9i	SUN SOLARIS	Existencia Combustible
Combustible	Oracle 9i	SUN SOLARIS	Obras Públicas Planificación Existencia
Sindicatura	Oracle 9i	SUN SOLARIS	Secretaría General Prefectura Obras Públicas Planificación Contabilidad - Presupuesto
Secretaría General	Oracle 9i	SUN SOLARIS	Prefectura Sindicatura
Auditoria	Oracle 9i	SUN SOLARIS	Contabilidad y presupuesto. Existencia Bodega de Proveeduría Combustible Recursos Humanos
Seguridad	Oracle 9i	SUN SOLARIS	Recursos Humanos

			Hardware
Hardware	Oracle 9i	SUN SOLARIS	Recursos Humanos Activos Fijos
Recursos Humanos	Oracle 9i	SUN SOLARIS	Contabilidad y Presupuesto.
Obras Públicas	Oracle 9i	SUN SOLARIS	Planificación Recursos Humanos Fiscalización Combustible
Concesiones	Oracle 9i	SUN SOLARIS	Recursos Humanos Combustible
Bodega de proveeduría	Oracle 9i	SUN SOLARIS	Compras y ruteo Existencia Activos fijos Contabilidad y presupuesto.
Brigadas Médicas	Oracle 9i	SUN SOLARIS	Existencia
Proyectos Especiales	Oracle 9i	SUN SOLARIS	Recursos Humanos Turismo Relaciones Públicas
Planificación	Oracle 9i	SUN SOLARIS	Obras Públicas Fiscalización Recursos Humanos Combustible
Sala de Comisiones	Oracle 9i	SUN SOLARIS	Prefectura Secretaría General
Seguros	Oracle 9i	SUN SOLARIS	Contabilidad y presupuesto. Existencia Activos fijos.

Relaciones Públicas	Oracle 9i	SUN SOLARIS	Prefectura
Turismo	Oracle 9i	SUN SOLARIS	Relaciones Públicas Proyectos Especiales
Fiscalización	Oracle 9i	SUN SOLARIS	Obras Públicas Fiscalización Recursos Humanos Combustible

CAPÍTULO II

ISO 17799

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ISO 17700 define la información como un activo que posee valor para la organización y requiere por lo tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños de la organización y maximizar el retorno de las inversiones y las oportunidades del negocio.

La seguridad de la información se define como la preservación de:
Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Integridad. Garantía de la exactitud y completitud de la información y los métodos de procesamiento.
Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

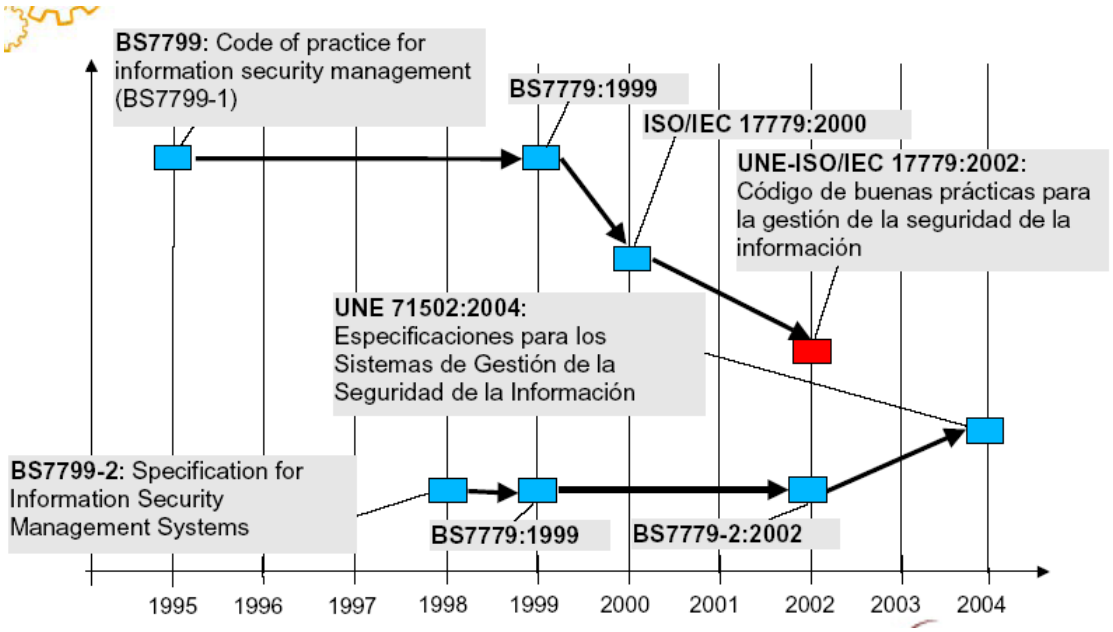
El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.
Es una norma no certificable, pero que recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI).

HISTORIA:

En 1995 el British Standard Institute publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información.
En 1996, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; la cual se revisa en 2002.
Tras una revisión de ambas partes de BS 7700 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
- Aplicable por toda organización, con independencia de su tamaño.
- Flexible e independiente de cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la tecnología.

En 2002 la norma ISO de adopta como UNE son apenas modificación (UNE 1977), y en 2004 se establece la norma UNE 71502, basada en BS7799-2 (no existe equivalente ISO).

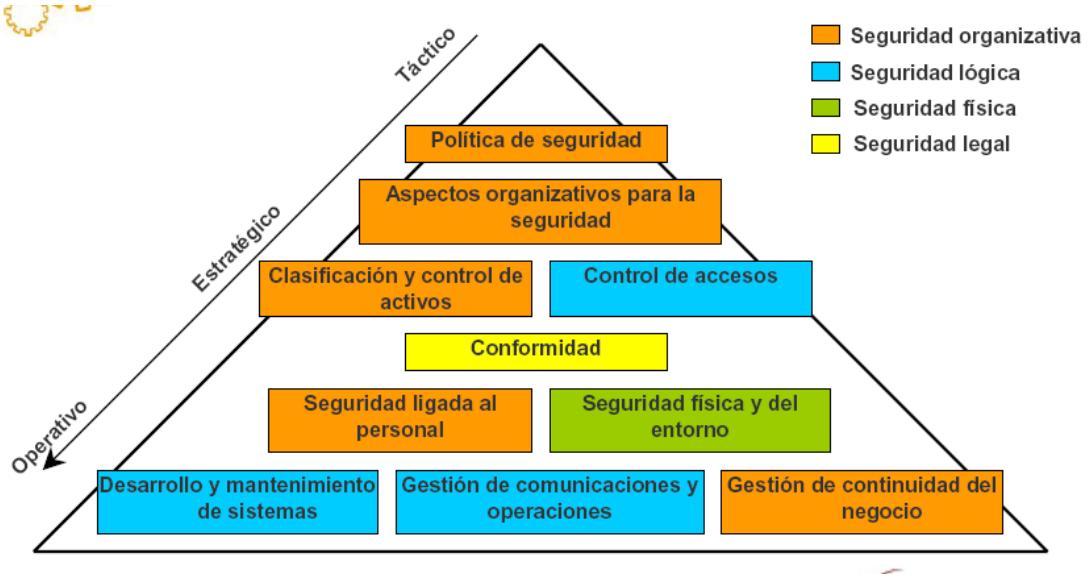


La norma ISO /IEC 17700 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad.
2. Seguridad de la Organización.
3. Clasificación y control de activos.
4. Seguridad del Personal
5. Seguridad física del entorno
6. Gestión de comunicaciones y operaciones
7. Control de acceso
8. Desarrollo y mantenimiento de los sistemas
9. Gestión de la continuidad del negocio
10. Cumplimiento.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

Estructura de los dominios de control



¿Por qué escoger ISO 17799 y no COBIT?

COBIT, lanzado en 1996, es una herramienta de gobierno de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de generales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. Misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores

Como hemos definido COBIT es un conjunto de controles generales para el gobierno IT, mientras ISO 17799 es una normativa internacional que contiene una guía de

controles y un conjunto de normas destinadas exclusivamente para la administración de la Seguridad de la Información. Por lo cual podemos decir que COBIT es un estándar general para los procesos relacionados IT, mientras ISO 17799 es un conjunto de normas y estándares relacionados con nuestro objetivo principal del proyecto y que corresponde a la salvaguardar de activos de información.

El presente proyecto tiene su base en ISO 17799: 2000, por considerarse relevante en la evaluación y definición de controles correspondientes a la seguridad de la información, por lo cual permite reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, además puede pasar por un proceso de auditoria para su certificación bajo la norma BS 7799 segunda parte y actualmente de UNE 71502.

Cabe mencionar que para el presente proyecto no se utilizó la norma de seguridad UNE 17502, ya que al momento de iniciar el proceso de tesis, esta norma no se encuentra disponible y accesible.

ANÁLISIS DEL ENTORNO TECNOLÓGICO DE LA INSTITUCIÓN.

Para efectos de analizar del entorno tecnológico de la Institución hemos utilizado la herramienta del Modelo de Madurez extraída de COBIT, la cual permitirá conocer la situación actual de la Institución y hacia donde se quisiera proyectar o que situación esperaría tener la organización en cuanto a seguridad de su ambiente tecnológico.

El modelo de madurez de CobiT ofrece las bases para el entendimiento y la evaluación de las condiciones actuales de seguridad y control de los procesos del ambiente de TI de una organización. Este modelo provee las bases para la evaluación de las principales funciones del área de TI, a través de la consideración de cada uno de sus procesos clave, a los cuales se les asignará un valor de cero (0) a cinco (5), según la definición que se muestra a continuación, indicando así el nivel de esfuerzo ("madurez") que se sugiere invertir en la actividad de control de dicho proceso, de forma de garantizar una buena relación costo beneficio al asegurar el nivel de seguridad estrictamente requerido. Las principales características que identifican a cada nivel son las siguientes:

0. Inexistente. Ausencia total de cualquier proceso o control reconocible. La organización no ha reconocido la necesidad del proceso o control.

1. Inicial. Existe evidencia de que la organización ha reconocido la necesidad de mejorar los procesos o controles. No existen procesos estandarizados, pero se realizan procedimientos "ad hoc" que tienden a aplicarse en casos individuales. La forma en que la gerencia enfrenta estos temas no se encuentra organizada.

2. Repetible. Se han desarrollado procesos donde se siguen procedimientos similares por diferentes personas para la misma tarea. No se ha formalizado la capacitación o la comunicación de los procedimientos en forma estándar, ni la responsabilidad es de cada individuo. Hay un alto grado de confianza en el conocimiento individual, por lo que los errores son más frecuentes.

3. Definido. Los procedimientos han sido estandarizados y documentados y son comunicados a través de la capacitación. Sin embargo, se deja a los individuos el

seguimiento de los procesos, por lo que resulta poco probable que se detecten desviaciones. Los procedimientos no son sofisticados pero existe formalización de las prácticas existentes.

4. Gestionado o administrado. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar acciones cuando los procesos no están funcionando efectivamente. Los procesos se encuentran constantemente bajo mejora y proveen buenas prácticas. Se utilizan automatización y herramientas de una forma limitada o fragmentada.

5. Optimizado. Los procesos han sido redefinidos al nivel de las mejores prácticas, basados en los resultados de mejoras continuas y el modelo de madurez con otras organizaciones. TI se utiliza de una forma integrada para automatizar el workflow, proveyendo herramientas para mejorar la calidad y la efectividad, con una rápida adaptación

Mejorando el nivel de madurez de los controles asociados a cada uno de los procesos de TI, según las necesidades reales de éstos, la organización logrará mejorar el nivel de control interno de los mismos. En este caso se obtendrán, al menos, un incremento de la eficiencia operativa y la formalización de los procesos.

Trabajando en base al modelo de madurez deseado, se seleccionarán los objetivos de control que deberán aplicarse a los efectos de evaluar la situación actual de cada uno de los procesos de TI de la organización. De esta manera se obtendrá el grado de cumplimiento de cada proceso tomando como marco de referencia los dominios provistos por la ISO/IEC 17799, pero guiados por los requerimientos reales de la organización.

El modelo de madurez representa entonces, "a dónde la organización desea llegar", mientras que el resultado de la evaluación representa "dónde la organización está". Las posibles brechas detectadas entre ambas situaciones serán los disparadores del plan de acción para implementar las soluciones que se requiera para mejorar la estructura de control interno en el grado deseado. De lo anterior se deduce que es tan

importante fijar adecuadamente "hasta dónde se desea llegar" (grado de madurez), cómo seleccionar los objetivos de control que permitirán realizar la evaluación.

El grado en el cual la institución desea llegar ha sido definido de acuerdo a las preocupaciones y visión de la máxima autoridad del área IT del H. Consejo Provincial del Guayas y la máxima autoridad de la Dirección Financiera; en reunión conjunta con todos los jefes departamentales de la Coordinación de Informática.

Cabe mencionar que la brecha significativa que existen entre la situación actual y esperada de los dominios ha sido factor preponderante para que la máxima autoridad del área IT, el Coordinador de Informática, defina los objetivos esperados en cuanto a la seguridad de la información para el año en curso, sobre todo en los siguientes dominios: Política de Seguridad, controles de acceso, seguridad física y ambiental, cumplimiento y seguridad organizacional.

Proceso ejecutado para medir el nivel de madurez:

De acuerdo a la Tabla 1.1. (Anexos) se realizó un análisis por dominio de la norma ISO 17799 y un programa de auditoria que permitió identificar el nivel de madurez actual de la Organización. A continuación se presentan los resultados de dicho programa de auditoria y el nivel esperado de la Organización con su respectiva justificación:

MODELO DE MADUREZ DEL H. CONSEJO PROVINCIAL DEL GUAYAS

A continuación la siguiente tabla presenta por dominio, el nivel actual en cual se encuentra la Institución con su respectiva justificación, se presenta así mismo el nivel esperado y los objetivos que se esperan cubrir con el mencionado nivel.

DOMINIO	NIVEL ACTUAL	JUSTIFICACIÓN	NIVEL ESPERADO	OBJETIVOS
Política de Seguridad	1 Inicial	- Política de seguridad no acorde con las necesidades institucionales. - Los usuarios desconocen los términos de la política de seguridad	4 Manejable y Mesurable	-Política de seguridad acorde con las necesidades organizacionales. - Existencia de procedimientos de inducción y capacitación de la política de seguridad, actualizaciones y modificaciones.

		y sus responsabilidades. - No existen procesos formales de inducción de la política de seguridad y capacitación sobre temas de seguridad al personal de la Organización.		- Personal o usuarios concientes y capacitados sobre temas de seguridad. - Existencia de procedimientos sobre reportes de incidentes y violación a la seguridad.
Organización de la Seguridad	0 Inexistente	- La organización no dedica tiempo y recursos al establecimiento de actividades básicas de soporte y operaciones de TI	3 Definido	- La necesidad de administrar operaciones de la computadora es atendida y aceptada dentro de la organización. - Se han asignado recursos y se lleva a cabo algún entrenamiento en el puesto de trabajo. - Las funciones repetibles están definidas formalmente, estandarizadas, documentadas y comunicadas al personal de operaciones y de clientes. - Los casos y resultados de tarea completados son registrados, pero el reporte a la administración es limitado o inexistente. - El uso de programación automatizada y de otras herramientas es extendido y estandarizado para limitar la intervención del operador. - Otras actividades regulares de soporte de TI están también definidas y se están definiendo las tareas relacionadas. - Se ejercen controles estrictos sobre poner en operación nuevos puestos de trabajo y se usa una política formal para reducir el número de casos no programados. - Monitoreo y control de los contratos de mantenimiento y de servicios con los vendedores aún son informales por naturaleza..
Clasificación y control de activos	1 Inicial	- Desconocimiento general sobre la importancia de los activos organizacionales.	3 Definido	- Existencia de procedimientos formales de inventario de activos de información. - Existencia de procedimientos de clasificación y etiquetado

		.- No existe inventario de activos real asociado con cada sistemas de información. - No existen clasificación de la información y controles asociados.		de la información.
Seguridad del personal	1 Inicial	- No existen responsabilidades claramente definidas del manejo de la seguridad, dichas responsabilidades no están documentadas en el manual de funciones. - No existen acuerdos de confidencialidad como términos y condiciones laborales del empleo. - No se especifican en los contratos con el personal términos relacionados a la seguridad.	3 Definido	- Existencia de responsabilidades claramente definidas con respecto a términos de seguridad. - Existirán acuerdos de confidencialidad en los contratos laborales.
Seguridad física y ambiental.	1 Inicial	- La organización reconoce la necesidad de estructurar las funciones de soporte deTI. - Sin embargo, no están establecidos procedimientos estándares y las actividades de operaciones son reactivas por naturaleza. - La mayoría de las operaciones no están formalmente programadas y las solicitudes de procesamiento son aceptadas sin validación previa. - Las computadoras que soportan los	3 Definido	- La necesidad de administrar operaciones de la computadora es atendida y aceptada dentro de la organización. - Se han asignado recursos y se lleva a cabo algún entrenamiento en el puesto de trabajo. - Las funciones repetibles están definidas formalmente, estandarizadas, documentadas y comunicadas al personal de operaciones y de clientes. - Los casos y resultados de tarea completados son registrados, pero el reporte a la administración es limitado o inexistente. - El uso de programación automatizada y de otras herramientas es extendido y estandarizado para limitar la intervención del operador.

		procesos de negocio son interrumpidas con frecuencia, demoradas o no están disponibles. - Se pierde tiempo mientras los empleados esperan recursos.		- Otras actividades regulares de soporte de TI están también definidas y se están definiendo las tareas relacionadas. - Se ejercen controles estrictos sobre poner en operación nuevos puestos de trabajo y se usa una política formal para reducir el número de casos no programados. - Monitoreo y control de los contratos de mantenimiento y de servicios con los vendedores aún son informales por naturaleza.
Control y comunicaciones y operaciones.	1 Inicial	- Se reconoce que los cambios deben ser administrados y controlados, pero no hay un proceso consistente para su control - Las prácticas varían y es probable que ocurran cambios no autorizados. - Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable. - Es probable que ocurran errores junto con interrupciones en el entorno de producción, causados por una administración deficiente de los cambios.	3 Definido	- Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, emergencia, autorización y administración de cambios, pero no se impone su cumplimiento. - El proceso definido no siempre es visto como adecuado o práctico y, en consecuencia, ocurren trabajos paralelos y los procesos son desviados. - Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.
Control de Accesos	1 Inicial	- Inexistencia de políticas de control de acceso. - los usuarios tienen restricciones mínimas en cuanto a privilegios. - la asignación de privilegios no es realizada de acuerdo a las funciones y	4 Manejable y Mesurado	- Existencia de procedimientos y políticas de control de acceso conocidas por todos los miembros de la Organización. - Existen responsabilidades claramente definidas en cuanto a control de acceso, supervisión y control. - Procedimientos expuestos y comunicados de manejo de claves, asignación y seguridad

		responsabilidades de los usuarios. - Los usuarios desconocen buenas prácticas de la asignación de contraseñas de seguridad. Los usuarios desconocen procedimientos que se aplican sobre equipos desatendidos. .- los usuarios no mantienen la confidencialidad de sus claves asignadas.		de las mismas.
Desarrollo y mantenimiento de los sistemas	2 Repetible e Intuitivo	- La conciencia de la necesidad de la exactitud de los datos y de mantener la integridad prevalece en toda la organización - La propiedad de los datos comienza a tener lugar, pero a nivel de un departamento o grupo. - Las reglas y requerimientos son documentados por personas claves y no son consistentes en toda la organización y plataformas. - Los datos están en la custodia de la función de los servicios de información y las reglas y definiciones están impulsadas por los requerimientos de TI. - La seguridad e integridad de los datos son primariamente responsabilidades de la función de los servicios de información con una	4 Manejable y Mesurado	- Los datos son definidos como un recurso y un activo corporativo, a medida que la administración exige más soporte de decisiones y más reporte de rentabilidad. - La responsabilidad por la calidad de datos está claramente definida, asignada y comunicada dentro de la organización. - Los métodos estandarizados están documentados, mantenidos, y usados para controlar la calidad de los datos, se hacen cumplir las reglas y los datos son consistentes en todas las plataformas y unidades de negocio. - La calidad de los datos y la satisfacción del cliente, es medida respecto a la información que es monitoreada. - El reporte de administración asume un valor estratégico para asesorar clientes, tendencias y evaluaciones de productos. - La integridad de los datos se vuelve un valor significativo, con la seguridad de datos reconocida como un requerimiento de control. - Se ha establecido una función formal de administración de datos a

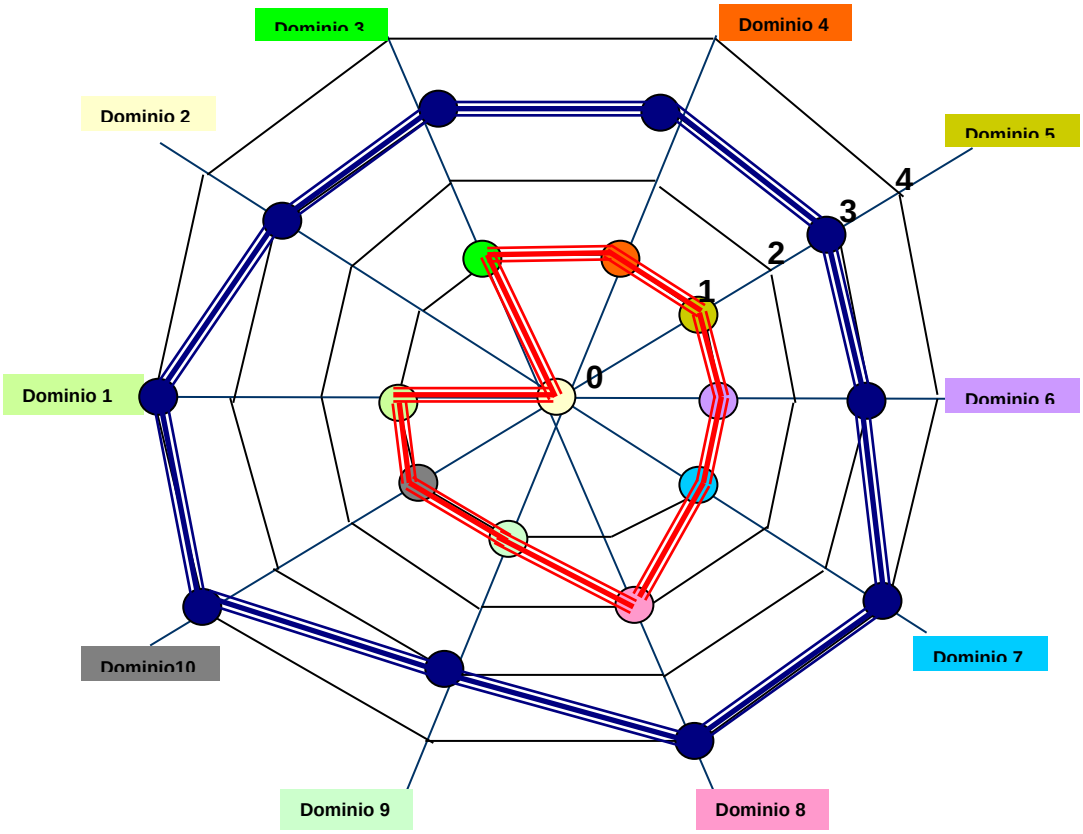
		participación departamental menor.		nivel de toda la organización, con los recursos y la autoridad para hacer cumplir la estandarización de datos.
Administración de la continuidad del negocio	1 Inicial	- Las responsabilidades de servicio continuo son informales, con autoridad limitada. - La administración se está volviendo conciente de los riesgos relacionados con servicio continuo y de la necesidad de éste. - El enfoque es sobre la función de TI, en vez de ser sobre la función de negocio. - Los usuarios están implementando formas de evadirlo. - La respuestas a las interrupciones mayores es reactiva e improvisada. - Los cortes planeados está programados para que satisfagan las necesidades de TI, en vez de adaptarse a los requerimientos del negocio.	3 Definido	- La obligación de reportar no es ambigua y las responsabilidades de planificar y probar el servicio continuo están claramente definidas y asignadas. - Los planes están documentados y se basan en la importancia del sistema y en el impacto sobre el negocio. - Hay un reporte periódico de prueba de servicio continuo. - Las personas toman la iniciativa para seguir las normas y recibir entrenamiento. - La administración comunica consistentemente la necesidad de servicio continuo. - Los componentes de alta disponibilidad y la redundancia de sistema se están aplicando de manera fragmentada. - Se mantiene rigurosamente un inventario de sistemas críticos y componentes.
Cumplimiento	1 Definido	- Desconocimiento de leyes y reglamentaciones por ciertos usuarios de la organización. - Existencia y utilización de software no legalizado. - falta de procedimientos que verifiquen el cumplimientos de leyes y reglamentaciones. - Inexistencias de función de auditoria interna.	4 Manejable y mesurado	- Sistemas organizacionales construidos de acuerdo a las leyes y ordenanzas gubernamentales. - Contratos elaborados con definiciones correctas de seguridad y cláusulas de confidencialidad de la información. - Existencia de procedimientos de auditorias que vigilen el cumplimiento de la seguridad de la información.

De acuerdo al nivel de Madurez presentado de la Institución, se puede observar que la misma en casi todos los dominios que detalla la norma ISO 17799:2000 se encuentra en un Nivel 1 o Inicial, esto quiere decir que la Institución podría estar atravesando significativos problemas de seguridad y que en la mayoría de los casos no existen procesos, procedimientos ni políticas documentadas y definidas correctamente.

Presentación Gráfica:

Modelo Actual Vs. Modelo Deseado

Como lo mencionamos anteriormente el nivel deseado ha sido definido por la máxima autoridad del área de IT, y la máxima autoridad a nivel de Dirección. (Director Financiero).



No.	DOMINIO	Situación Actual	Modelo Deseado
1	POLÍTICA DE SEGURIDAD	**1**	4
2	ORGANIZACIÓN DE LA SEGURIDAD	**0**	3
3	CLASIFICACIÓN Y CONTROL DE ACTIVOS	**1**	3
4	SEGURIDAD DEL PERSONAL	**1**	3
5	SEGURIDAD FÍSICA Y AMBIENTAL	**1**	3
6	GESTIÓN DE COMUNICACIONES Y OPERACIONES	**1**	3
7	CONTROL DE ACCESOS	**1**	4
8	DESARROLLO Y MANTENIMIENTO DE SISTEMAS	**2**	4
9	ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS	**1**	3
10	CUMPLIMIENTO	**1**	4

ANÁLISIS DE RIESGOS

INTRODUCCIÓN.-

Con los resultados proporcionados por el modelo de madurez a continuación se realizará el Análisis de Riesgo, tomando en cuenta todos los dominios con sus respectivos objetivos de control, luego se procede a identificar los riesgos por cada uno de ellos con la ayuda de los miembros de directivas de los altos niveles, y para finalizar se realiza su respectiva evaluación.

Con la ayuda de esta metodología, nosotros tendremos una visión mucho más clara sobre la situación actual en la que se encuentra la institución, y así podremos identificar los dominios de nivel de riesgo más severos.

EXPLICACIÓN DE LA METODOLOGÍA.-

Para un mejor entendimiento en la documentación se utilizó el siguiente cuadro para el respectivo Análisis de Riesgo:

Dominios a Evaluar

Objetivos de Control correspondientes a ese dominio, las cuales están descritas en la Norma.

Riesgos Identificados por cada objetivo de control, con la ayuda de la alta dirección.

Dominio	Objetivos de Control	RIESGOS	Evaluación del Riesgo			
			Probabilidad	Impacto	Ponderacion	Nivel de Riesgo
Política de Seguridad	Política de Seguridad de Información	Poco compromiso de la gerencia	6	8	48	
		Falta de apoyo al área de informática	6	8	48	
		Desconocimiento de los usuarios sobre la importancia de seguridad de la información	6	8	48	
		Políticas descontinuadas y no acordes al cambio de tecnologías.	4	6	24	
Organización de la Seguridad	Infraestructura de seguridad de información	Proyectos no culminados de forma satisfactoria	4	7	28	
		Objetivos de seguridad no alineados con los objetivos del negocio	4	7	28	
		Toma de decisiones equivocadas con respecto a la seguridad de los activos de la empresa	5	7	35	

Probabilidad e Impacto se evalúa en base de los siguientes parámetros:
0-2 Bajo
3-5 Medio
6-8 Alto

Cálculo : Probabilidad * Impacto

Nivel de Riesgo, representado por los colores del semáforo, cuyos parámetros de evaluación son los siguientes:

Equivalencias Nivel de Riesgo			
48	64	Alto	
25	47	Medio	
1	24	Bajo	

DESARROLLO

MATRIZ DE ANÁLISIS DE RIESGOS DEL H. CONSEJO PROVINCIAL DEL GUAYAS

Dominio	Objetivos de Control	RIESGOS	Evaluación del Riesgo			
			Probabilidad	Impacto	Ponderación	Nivel de Riesgo
Política de Seguridad	Política de Seguridad de Información	Poco compromiso de la gerencia	6	8	48	
		Falta de apoyo al área de informática	6	8	48	
		Desconocimiento de los usuarios sobre la importancia de seguridad de la información	6	8	48	
		Políticas descontinuadas y no acordes al cambio de tecnologías.	4	6	24	
Organización de la Seguridad	Infraestructura de seguridad de información	Proyectos no culminados de forma satisfactoria	4	7	28	
		Objetivos de seguridad no alineados con los objetivos del negocio	4	7	28	
		Toma de decisiones equivocadas con respecto a la seguridad de los activos de la empresa	5	7	35	
		Responsabilidades no se encuentran claramente identificadas	6	7	42	
	Seguridad del acceso de terceras personas	Accesos físicos no autorizados de terceras personas	7	8	56	

		Accesos lógicos no autorizados de terceras personas	8	8	64	
		Contratos con terceros no especifican requerimientos de seguridad, acuerdos de confidencialidad	8	8	64	
Clasificación y Control de Activos	Responsabilidad por los Activos	Protección inadecuada de los activos de información	4	6	24	
		Pérdida de confidencialidad de la información	4	6	24	
	Clasificación de la información	Falta de identificación de información pública y confidencial	4	6	24	
Seguridad del Personal	Seguridad en la definición del Trabajo y la asignación de recursos	Error humano en tareas críticas debido a selección inadecuada de personal	5	6	30	
		Robo o fraude por falta de acuerdos de confidencialidad y definición de responsabilidades de seguridad	4	6	24	
		Uso inadecuado de las instalaciones	5	5	25	
	Capacitación del Usuario	Pérdida de integridad de la información debido a desconocimiento de procesos	3	7	21	
		Errores y fallas en los ingresos de datos	5	7	35	

	Responder a los incidentes y malfuncionamientos en la seguridad	Tiempo de respuesta alto en la solución de problemas por falta de registros de incidentes	7	6	42	
		Violación de las políticas y procedimientos de seguridad de forma reiterada	5	8	40	
Seguridad Física y Ambiental	Áreas de seguridad	Accesos no autorizados a lugares de procesamiento de información	6	8	48	
		Robo, pérdida y modificación de la información y activos.	6	8	48	
	Seguridad del Equipo	Daños e intrusiones	6	8	48	
		Pérdida de información por fallas eléctricas	6	8	48	
		Daños de equipos por ubicación: Incendio, robos, vibraciones, polvo, humo, agua y comidas y bebidas.	7	8	56	
		Daños de equipos o pérdida de integridad de la información por fallas en el suministro de energía u otras anomalías eléctricas	6	8	48	
		Accesos no autorizados a los cuartos de telecomunicaciones	4	7	28	
		Incremento en costo de los equipos por reposición de partes y piezas averiadas por falta de mantenimiento	7	6	42	

	Controles Generales	Divulgación, modificación o robo por personas no autorizadas	4	8	32	
		Retiros no autorizados de propiedad	3	8	24	
Gestión de Comunicaciones y Operaciones	Procedimientos y Responsabilidades Operacionales	Ejecución de cambios no autorizados	3	8	24	
		Desconocimiento de las operaciones correctas por cambio no documentados ni comunicados	5	8	40	
		Fallas en los sistemas de información	5	7	35	
		Pérdida de continuidad del servicio	3	6	18	
		Violación de la confidencialidad de la información	4	7	28	
	Planeación y Aceptación del sistema	Fallas de integridad de la información procesada por los sistemas	4	7	28	
		Mal uso del sistema por la falta de segregación de funciones	6	6	36	
		Sistemas no acordes con las necesidades Institucionales	5	7	35	
		Errores resultantes de los ingresos incompletos e inexactos	6	7	42	
		Accesos no autorizados a los sistemas activos e información	5	7	35	
		Sobrecarga de los sistemas de información	5	7	35	

	Protección contra software malicioso	Introducción de código no autorizado o alteración de la información por no-separación del ambiente de desarrollo y producción	3	7	21	
	Gestión en casa	Embargo por utilización de software no autorizado	3	8	24	
		Pérdida de integridad de la información	4	8	32	
		Pérdida de la disponibilidad de la información	4	8	32	
		Daños en las cintas, discos y medios de respaldo o backup de información	4	8	32	
	Administración de Redes					
	Administración y Seguridad de Medios	Divulgación de información no autorizada y mal uso	4	7	28	
		Accesos no autorizados	4	7	28	
	Intercambio de información y software	Pérdida, modificación o mal uso de la información	4	7	28	
		Desconocimiento de responsabilidades en el evento de pérdida de información	6	7	42	
		Accesos no autorizados, mal uso o corrupción durante el transporte físico	4	7	28	
		Divulgación o modificaciones de la información no autorizadas	4	7	28	

Control de Accesos	Control de acceso	Accesos no autorizados a la información de la organización de acuerdo a las necesidades de seguridad del negocio	4	8	32	
	Administración del acceso del usuario	Accesos, privilegios y eliminación de usuarios sin autorización	6	8	48	
	Responsabilidad del usuario	Accesos no acordes con la política de seguridad organizacional	7	8	56	
		Falta de rastros o registros para identificar los accesos no autorizados	7	8	56	
		Fallas en los sistemas por asignación inapropiada de privilegios de los usuarios a los sistemas	5	8	40	
		Acceso de usuarios no autorizados debido a la pérdida de confidencialidad de claves	8	8	64	
		Mal uso de clave de acceso por parte de los usuarios	7	8	56	
		Divulgación, pérdida y robo de información por equipos desatendidos en áreas de usuarios	7	8	56	
	Control de acceso a redes	Accesos no autorizados a los servicios de red	5	8	40	
		Conexiones inseguras que provocan lentitud y mala gestión de la red	4	8	32	
		Falta de autorizaciones a los servicios de red	4	7	28	
		Pérdida de confidencialidad de la información por accesos no autorizados a los servicios de red	5	8	40	

	Control de Acceso al Sistema de Operación	Accesos no autorizados al Sistema Operativo	7	7	49	🔴
		Falta de registros para identificar la identidad de accesos.	7	7	49	🔴
	Control de Accesos a la aplicación.	Accesos no autorizados a la información generada por los sistemas de información	5	8	40	🟡
		Divulgación de información confidencial	5	8	40	🟡
		Pérdida, robo y modificación de la información	5	8	40	🟡
	Acceso y uso de sistema de monitoreo.	Ejecución de actividades no autorizadas	4	8	32	🟡
		Violación de la política de control de accesos	4	8	32	🟡
		Inexactitud de los registros de auditoria	3	8	24	🟢
	Computación móvil y Telecommuting.	Intromisión de software malicioso	5	7	35	🟡
		Accesos no autorizados por medio de computación móvil	2	7	14	🟢
		Divulgación de información sensible por accesos remotos no autorizados	4	8	32	🟡
Desarrollo y Mantenimiento de Sistemas	Requerimientos de Seguridad de los Sistemas.	Aplicaciones no acorde con las necesidades Institucionales	4	7	28	🟡
		Análisis incorrecto y aplicaciones poco funcionales	4	7	28	🟡

	Seguridad en los Sistemas de Aplicación.	Pérdida, modificación o mal uso de la información de los sistemas de información	4	8	32	
		Pérdida de integridad de la información	4	7	28	
	Seguridad de los archivos del sistema.	Información inconsistente	4	8	32	
		Pérdida de integridad de la información de los sistemas de aplicación	4	8	32	
		Corrupción de los sistemas operacionales	4	8	32	
		Mal uso de las bases de datos operacionales	5	8	40	
	Seguridad en los procesos de desarrollo y apoyo.	Corrupción de los programas fuentes	4	8	32	
		Software y aplicaciones no seguras	4	8	32	
		Pérdida de integridad de los sistemas de aplicación	4	8	32	
		Pérdida de disponibilidad y confidencialidad	4	8	32	
Administración de la Continuidad del Negocio	Aspectos de la gestión de la Continuidad del Negocio.	Interrupciones de las actividades de la organización	3	7	21	
		Fallas de seguridad debido a desastres naturales, accidentes o fallas de equipos	5	7	35	
		Plan de Continuidad ineficientes o sin cumplir objetivos principales del negocio	4	7	28	

		Plan discontinuado	4	7	28	
		Daños o incidentes que afecten la seguridad de la información y la continuidad del negocio	5	7	35	
Cumplimiento	Cumplimiento con requerimientos legales.	Violaciones de leyes de derecho civil y penal	3	8	24	
		No cumplimiento con los requisitos legales de seguridad	3	8	24	
		Embargos de activos por incumplimiento de propiedad intelectual	3	8	24	
		Multas y penalidades por incumplimiento de ley	5	6	30	
		No asignación de recursos por parte del Estado	5	6	30	
		Privación de Libertad de funcionarios responsables de infracciones	3	6	18	

Equivalencias Nivel de Riesgo			
48	64	Alto	
25	47	Medio	
1	24	Bajo	

CAPÍTULO III

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA

PARA EL H. CONSEJO PROVINCIAL DEL GUAYAS

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA

El enfoque del Plan del Sistema de Gestión de Seguridad de Información (SGSI) para el presente proyecto es evaluar aquellos dominios y objetivos de control más críticos, resultantes del análisis de riesgo realizado.

Esto quiere decir que una vez realizado el Modelo de Madurez para identificar la situación actual y después de haber recogido las preocupaciones de la gerencia y haber realizado el correspondiente análisis de riesgos de la Institución, se identificaron los dominios y objetivos de control más críticos para la organización.

El Alcance del SGSI del H. Consejo Provincial del Guayas estará definido por evaluar aquellos dominios identificados como más críticos para la Institución, con el objetivo de minimizar los riesgos en cuanto a seguridad de la información; los dominios se mencionan a continuación:

- Política de seguridad de la información.
- Organización de la seguridad.
- Control de Accesos.
- Seguridad Física y Ambiental.

Como parte del alcance del Sistema de Gestión de Seguridad de la Información para el H. Consejo Provincial del Guayas, se realizará una declaración de aplicabilidad; la cual definirá todas aquellas recomendaciones y controles sugeridos para cada dominio son aplicables para la Organización, y como parte final se propondrá un plan de acción recomendado para que el H. Consejo Provincial del Guayas implemente el conjunto de recomendaciones sugeridas a través de la evaluación y especificadas en el Sistema de Gestión de Seguridad de la Información.

Alcance geográfico:

El plan del SGSI se realizará sobre los activos de información ubicados en el edificio matriz del Honorable Consejo Provincial del Guayas, situado en la ciudad de Guayaquil en las calles Illingworth y Malecón Simón Bolívar.

Los objetivos específicos del diseño del Sistema de Gestión de Seguridad Informática es el siguiente:

- Evaluar los controles existentes con respecto a la política de seguridad de la información, analizar y recomendar los controles inexistentes o compensatorios que coadyuven el establecimiento de normas de seguridad especificadas mediante una política de seguridad.
- Definir los lineamientos, normas, procesos y controles que deberían observarse en la Política de Seguridad de la Información para el H. Consejo Provincial del Guayas, realizando un documento formal que servirá como guía a la Institución para la adecuada estructura de la Política de Seguridad.
- Evaluar los controles existentes en cuanto a accesos de terceros a la Institución, definir las recomendaciones, controles inexistentes, controles que recitasen ser rediseñados u otros controles compensatorios que coadyuven con la seguridad de la información.
- Evaluar los controles existentes de accesos mediante los sistemas operativos usados por usuarios finales en la Institución, definir aquellos controles inexistentes o compensatorios, o en su defecto aquello controles que necesiten ser rediseñados para que permitan minimizar los riesgos de divulgación, robo y pérdida de integridad de la información.
- Evaluar los controles existentes con respecto Seguridad Física y Ambiental de la Institución, con la finalidad de recomendar controles inexistentes, compensatorios o efectuar un rediseño de los ya existentes para garantizar la seguridad esperada.
- Realizar la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información.
- Proponer un plan de acción para la implementación del Sistema de Gestión de la Seguridad de la Información.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

Objetivo:

La Política de la Seguridad de la Información tiene como objetivo dar soporte a la gestión de la seguridad de la información.

Desarrollo:

Para el presente proyecto se ha definido el conjunto de lineamientos y normas en referencia a procesos y procedimientos, dichos lineamientos mínimos requeridos se encuentran definidos y documentados en la Política de Seguridad de la Información; así como los niveles de responsabilidad adecuados para garantizar los objetivos de seguridad de la información esperados.

A continuación detallamos la Política de Seguridad de la Información para el H. Consejo Provincial del Guayas.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

Introducción:

El H. Consejo Provincial del Guayas cuenta con sus dependencias centrales ubicadas en Malecón e Illingwoth esquina y sus oficinas anexas ubicadas en Plaza Dañín y Pedro Menéndez Gilberth. La Institución inicio su proceso de automatización desde el año 2000, desde el cual han surgido necesidades crecientes relacionadas al aspecto tecnológico e informático; el cual abarca todo lo relacionado a equipamiento del centro de cómputo y usuarios finales, redes, operaciones, aplicaciones y sistemas de información.

Con los procesos crecientes de información, la Institución tiene la necesidad de salvaguardar de forma correcta los activos de información y el equipamiento informático existente; para así protegerlos de cualquier amenaza y minimizar los riesgos de accesos no autorizados, fraudes, robos, sabotajes y mal uso de la información Institucional.

La información Institucional debe protegerse y en referencia a ello, la presente política contendrá todos los lineamientos necesarios para establecer la seguridad adecuada sobre los activos y la información de la Organización. Así mismo cabe mencionar que la implementación de esta política de seguridad de la información es responsabilidad de todos los miembros de la organización y como tal debe ser transmitida a los Directores, Subdirectores, Jefes departamentales y seccionales y a todos los miembros de la Organización en general.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

El diseño de la Política de Seguridad de la Información del H. Consejo Provincial del Guayas está basado en el Estándar Internacional ISO/IEC 17799, considerando los dominios y objetivos de control más significativos y que aseguren los parámetros adecuados de seguridad de la Organización.

OBJETIVO GENERAL DE LA POLÍTICA DE SEGURIDAD

Establecer las directrices y lineamientos necesarios para obtener una adecuada y acorde seguridad de los activos y de la información institucional.

ALCANCE:

La presente política establece las directrices y lineamientos de seguridad sobre los siguientes puntos:

- Definición, documentación y divulgación de la Política de Seguridad de la Información.
- Políticas concernientes a la clasificación y el control de los activos.
- Políticas de seguridad organizacional.
- Políticas de seguridad física y del entorno.
- Políticas de la Comunicación y de las Operaciones.
- Políticas del Control de Acceso.
- Políticas con respecto al Desarrollo y Mantenimiento de los sistemas.
- Políticas de Continuidad del Negocio.
- Políticas del Cumplimiento y control.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

RESPONSABILIDADES:

Coordinador de Informática: Responsable de supervisar el proceso de implementación de las políticas, controles y procedimientos de seguridad descritos en la presente política. Es responsable de sugerir, evaluar y decidir sobre temas relacionados a la seguridad del ambiente y entorno institucional en lo referente a conservar los principio de integridad, disponibilidad y confidencialidad de la información.

Jefe de Seguridad: Responsable del diseño e implementación de los controles necesarios para conservar la integridad, disponibilidad y confidencialidad de la información, así mismo como de establecer mecanismos y procedimientos de seguridad adecuados y acordes con los intereses Institucionales; así como dirigir y ejecutar mecanismos de comunicación y divulgación sobre la política y procedimientos de seguridad implementados.

Administrador de Red: Será responsable de la implementación de los controles con respecto al área de operaciones, redes y sistemas operativos; e informar cualquier incidente, intento o violación a la seguridad al Jefe de Seguridades. El administrador de la red será responsable de monitorear las actividades de los usuarios y monitorear las capacidades de los recursos del sistema.

Usuarios:

Los usuarios serán responsables en principios generales de:

- Leer y conocer la política, procedimientos y normas de seguridad informática de la Institución.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Ejecutar y aplicar los procedimientos de seguridad descrito en la presente política.
- No divulgar información institucional.
- No permitir el ingreso de personas no autorizadas al equipo de procesamiento de información.
- No revelar sus usuarios y contraseñas bajo ningún concepto.
- Velar por el buen uso de los bienes informáticos.
- Reportar inmediatamente a su jefe inmediato o jefe de seguridades institucionales cualquier intento o violación a la seguridad observada o sospechada.

LEYES QUE RIGEN LA PRESENTE POLÍTICA DE SEGURIDAD

- Constitución Política de la República del Ecuador
- Código del Trabajo del Ecuador
- Ley Especial de Descentralización
- Ley de Modernización del Estado y Privatizaciones
- Ley de presupuesto nacional del estado.
- Ley del Régimen Provincial
- Ley Orgánico de Servicio Civil y Carrera Administrativa
- LOAFIC (Ley Orgánica de Administración Financiera y Control)
- Reglamento a la ley de descentralización
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley de control y reglamentación de bienes del sector público.
- Políticas internas del personal
- Normas y procedimientos internos de la Institución.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN:

Objetivo: Brindar orientación y apoyo a la de la dirección para la seguridad de la información.

Políticas:

La Política de Seguridad de la Información debe:

- Ser revisada y aprobada por la máxima autoridad Institucional.
- Estar debidamente documentada, publicada y comunicada a todos los empleados.
- Ser publicada en un medio de fácil acceso para todos los miembros de la Organización (Intranet) y divulgada a través de los servicios informáticos como correo electrónico y red Institucional.
- Ser entregada como documento formal por la Dirección de Recursos Humanos al momento de contratación de personal nuevo a la Institución.

POLÍTICAS DE LA SEGURIDAD ORGANIZACIONAL

Objetivo:

- Gestionar la seguridad de la información dentro de la Organización.
- Mantener la seguridad de las instalaciones de procesamiento de la información organizacional y los activos de información a las que tienen acceso terceras partes.

Políticas:

- La Institución deberá contar con un comité sobre la seguridad de la información, quienes serán responsables de obtener los compromisos

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- necesarios y los recursos apropiados para mantener la correcta seguridad de los activos y de la información Institucional.
- Se deberá formar comités interfuncionales de seguridad con representantes de las diferentes áreas con la finalidad de coordinar la implementación de los controles de seguridad de la información
- Las responsabilidades para la protección de los activos individuales serán definidas a través de las tenencias legalizadas de los Bienes de la Institución.
- El responsable de velar por la seguridad, custodio y buen uso de la información, será el encargado de la Seguridad Informática de la Institución.
- Los cambios de los ambientes o lugares de procesamiento de la información serán conocidos, evaluados y aprobados por el comité de seguridad de la información.
- La Institución deberá aplicar los respectivos mecanismos de control en el acceso de terceros a las dependencias.
- En el caso que los servicios de terceros incluyan el uso de las dependencias y recursos de la Institución; los terceros deberán comprometerse a mantener los recursos asignados en buen estado o en su defecto en el estado que les fueron asignados.
- En el caso de acceso de terceros que presten servicios tecnológicos deberán ser plenamente identificados por el personal de control de acceso al edificio, llevando un registro del personal que ingresa y el lugar del edificio al cual han accedido para la ejecución de las responsabilidades.
- El acceso de terceros a las instalaciones fuera del área de la Coordinación de Informática, deberá ser llevado a cabo de forma obligatoria en compañía como

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- mínimo de una persona del departamento de mantenimiento del edificio y una persona mínima del área de la Coordinación de Informática.
- Los contratos de servicios con terceros deberán contener los correspondientes niveles de servicios y condiciones de seguridad adecuadas.
- Si el servicio de terceros contemplase actividades relacionadas al manejo, generación, salvaguarda y administración de información Institucional, los contratos deberán poseer las correspondientes cláusulas de confidencialidad de la Información, con las respectivas penalidades en caso de violación de las mismas.

POLÍTICAS DE SEGURIDAD Y CONTROL DE ACTIVOS

Objetivos:

- Mantener la protección adecuada de los activos organizacionales.
- Asegurar que los objetivos de información reciben el nivel de protección adecuada.

Políticas:

- Se deberá elaborar y mantener un inventario de todos los activos asociados con cada uno de los sistemas de información.
- Todos los activos relacionados al procesamiento de información y de datos serán correctamente identificados y etiquetados.
- Deberá existir un procedimiento para la clasificación de la información de tal forma que se considere por lo menos dos parámetros de clasificación de la información: privada (confidencial) y pública.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Los usuarios son responsables de los activos de procesamiento de información que se encuentren respectivamente documentados, registrados y legalizados en las tenencias de bienes de la Institución.

POLÍTICAS DE SEGURIDAD DEL PERSONAL

Objetivos:

- Reducir los riesgos de error humano, robo, fraude o uso inadecuado de las instalaciones.
- Asegurar que los usuarios tengan conciencia sobre las amenazas y problemas de seguridad de la información y que estén preparados para brindar apoyo a la política de seguridad de la información organizacional en el curso de su trabajo normal.
- Minimizar el daño causado por incidentes y anomalías en materia de seguridad, hacer el seguimiento y aprender de estos incidentes.

Políticas:

- Las funciones y responsabilidades de seguridad descritas al inicio de la política de seguridad, deben estar documentadas en la definición de cargos y manual de funciones de la institución.
- El Coordinador de Informática es responsable de ejecutar procedimientos de evaluación del personal al momento de su ingreso así como de su desempeño laboral.
- El Coordinador de Informática deberá intervenir en la evaluación del personal de terceros que prestasen servicios dentro de la Institución.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Los contratos del personal que laborasen en el área de tecnología y funciones afines deberán contener cláusulas de confidencialidad de la información.
- Los términos y condiciones de la relación laboral deben indicar la responsabilidad de los empleados en cuanto a la seguridad de la información.
- Los empleados de la institución, así como personal externo y tercializado deben recibir la formación adecuada y las actualizaciones regulares sobre las políticas y procedimientos organizacionales.
- Los procedimientos para el reporte de incidentes deben ser conocidos por todos los miembros de la organización.
- Los usuarios deben conocer los procedimientos para el reporte de anomalías de software. Los procedimientos deben incluir el reporte de incidentes sobre cualquier debilidad en la seguridad, observada o sospechada, o amenazas a los servicios y sistemas.
- El usuario no deberá ingerir ni alimentos ni bebidas cerca de los equipos de computación, con la finalidad de evitar daños a los mismos o pérdida de información.
- El Director de Recursos Humanos o Jefe de cada área deberá comunicar a la Coordinación de Informática la salida temporal (vacaciones, permisos por enfermedad, permisos por lactancia, etc.) o salida definitiva de cualquier persona que posea una cuenta de usuario, para proceder a su bloqueo inmediato o eliminación. Dicho proceso debe estar sustentando y legalizado en el formulario de acceso a la red o de acceso a los sistemas.
- Los equipos de La compañía sólo deben usarse para actividades de trabajo y no para otros fines, pasatiempos o asuntos personales.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivos:

- Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones a las instalaciones e información de la empresa
- Evitar daño, pérdida o puesta en peligro de los activos e interrupción de las actividades de la organización.
- Evitar el robo de la información de las instalaciones de procesamiento de información y evitar que ésta quede expuesta a algún peligro,

Políticas:

- El perímetro de seguridad de las áreas de procesamiento de la información deberá estar correctamente vigilado y supervisado.
- Las áreas de procesamiento de la información deberán tener controles de entradas y salidas magnéticos que garanticen registros de visitas de personal interno como externo.
- No se permitirá el ingreso de personal no autorizado a las áreas de procesamiento de la información.
- Los equipos deben estar correctamente protegidos para reducir los riesgos de amenazas o peligros del entorno y los accesos no autorizados.
- Los equipos deben estar correctamente protegidos contra fallas en el suministro de energía y otras anomalías eléctricas.
- Cuando ocurra alguna falla o ante la falta de energía eléctrica el usuario deberá cerrar todas las aplicaciones y apagar los equipos de manera inmediata.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Los equipos deben recibir el adecuado mantenimiento de forma periódica que permitan su permanente disponibilidad e integridad.
- La instalación de cualquier clase de programas, el chequeo, mantenimiento y reparación de los equipos de computación, son competencia del personal de la Coordinación de Informática.
- La salida de cualquier equipo informático de la Institución debe ser autorizada por la Dirección a la cual pertenece el equipo y por la Coordinación de Informática.
- El personal del departamento de mantenimiento y seguridad de la Institución deberá llevar un registro y control de los equipos informáticos que entran y salen de la Institución.
- Al momento de traspasar de un usuario a otro un equipo de computación, la información contenida en este debe ser eliminada o destruida.
- La información de los equipos que son dados de baja deberá ser destruida o eliminada.
- Todas las computadoras deben poseer mecanismos de bloqueo manuales o automáticos tanto de sistemas operativos como de las aplicaciones, y controles automáticos de bloqueo por inactividad del equipo.
- Los usuarios deberán cerrar sesión, bloquear equipos o activar protector de pantalla cada vez que dejen inactivo su computador.
- Al terminar la jornada el usuario deberá colocar correctamente los cobertores asignados para sus equipos, en caso de tenerlos

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

POLÍTICAS DE GESTIÓN DE REDES Y OPERACIONES

Objetivo:

- Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de la falla de los sistemas.
- Mantener la disponibilidad e integridad de los servicios de comunicación y procesamiento de la información.
- Evitar el daño a los activos, y las interrupciones en la actividad de la Organización.
- Evitar la pérdida, modificación o uso inadecuado de la información intercambiada entre organizaciones.

Políticas:

- Toda computadora de la Institución que cuente con cableado estructurado y capacidades adecuadas debe estar conectada a la red Institucional.
- Se deberán seguir los procedimientos necesarios para los cambios en las instalaciones y sistemas de procesamiento de información; de tal forma que garanticen la seguridad y funcionamiento adecuado después de la ejecución de dichos cambios.
- Los responsables de manejo de incidentes serán cada Jefe de Área de la Coordinación de Informática, y deberán mantener un registro con el fin de asegurar una respuesta rápida, eficaz y sistemática a los problemas de seguridad.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Las funciones y áreas de responsabilidad deben estar correctamente separadas, identificadas y documentadas en el manual orgánico funcional de la Institución.
- Las funciones de desarrollo y producción deberán separarse, formando para ello dos ambientes uno de desarrollo y otro de producción.
- Deberán existir procedimientos adecuados para controlar los cambios en el desarrollo del software, que son llevados de ambiente de desarrollo a producción.
- Previa evaluación y justificación del software requerido por el usuario o el departamento, la Coordinación de Informática se encargará de la instalación del mismo. Se recuerda que todo programa no autorizado por la Coordinación de Informática, será inmediatamente eliminado y se reportará al Jefe inmediato.
- Se deberán realizar seguimientos a las demandas de capacidad y se deberán hacer continuas proyecciones de la capacidad futura, para posibilitar la disponibilidad de recursos de procesamiento y almacenamiento necesario.
- Deberán existir procedimientos para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones. Dicha aceptación deberá ser legalizada mediante un documento formal (Acta de Entrega/Recepción) por el Coordinador de Informática y el usuario principal dueño de la aplicación.
- La institución deberá contar con un procedimiento formal de detección y prevención contra software malicioso.
- No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Institución a menos que se haya verificado en primera instancia que están libres de virus u otros agentes dañinos

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- El procedimiento descrito para prevenir la intromisión de software malicioso deberá ser comunicado a todos los usuarios de la Institución y deberá estar publicado en la intranet institucional.
- Se deberán ejecutar los mecanismos de respaldos apropiados que garanticen el resguardo de información.
- Los respaldos de la información serán ejecutados en cintas magnéticas de calidad probada y garantizada.
- Dichos respaldos se ejecutarán de forma diaria y semanal, produciéndose tres copias del mismo; las cuales serán almacenadas de la siguiente forma: una permanecerá en un lugar seguro de resguardo de información dentro del departamento de la Coordinación de Informática, una segunda copia en un lugar seguro dentro de la Institución y una tercera copia deberá ser almacenada en un lugar externo a la organización y será conocido por el Jefe de Seguridades, Coordinador de Informática y la máxima autoridad.
- Deberá existir un procedimiento para ejecutar las respectivas pruebas de las cintas de respaldo. Dichas pruebas deberán ser certificadas por el Coordinador de Informática y el Jefe de Seguridades.
- El personal del centro de cómputo deberá mantener una bitácora (log) de sus actividades. Estos registros deben ser revisados regularmente por el responsable de las seguridades de la Información.
- Se deberá tener una bitácora de fallas de las actividades de operación, y deberá llevarse así mismo el registro de las acciones correctivas y los mecanismos o actividades para la solución de dichas fallas.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- El usuario no podrá acceder a opciones de configuración del computador, por lo tanto no podrá compartir recursos en red como drivers, carpetas etc. En el caso de las impresoras podrán compartirse para la utilización del personal del mismo departamento con la autorización previa del Director del área,
- El usuario no podrá modificar, cambiar o alterar el papel tapiz de la Institución, configurado en cada estación de trabajo.
- Deberá existir un procedimiento de control sobre los medios de computación removibles tales como cintas, casetes, discos, reportes impresos y dispositivos de almacenamiento externo.
- Deberá existir un procedimiento para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación o acceso no autorizado.
- La documentación generada de los sistemas, así como la documentación en lo referente a manuales de análisis, diseño y de usuario, deberá estar protegida con la finalidad de evitar acceso no autorizado.
- Cualquier medio en tránsito debe protegerse contra acceso no autorizado, uso inadecuado, manipulación y corrupción.
- El control de acceso será regulado por la siguiente política:
    - El procedimiento formal para el registro de usuarios a la red y las aplicaciones institucionales se llevará a cabo a través de "solicitudes de acceso a la red" y "solicitudes de acceso a los sistemas" en la cual se establecen los parámetros correspondientes para la adición, eliminación o suspensión de usuarios a los servicios mencionados.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Se deberá controlar la asignación y uso de privilegios de red y de los sistemas por medio de controles del sistema operativo y de las aplicaciones.
- Las computadoras funcionarán únicamente mediante el uso de un nombre de usuario (login) y contraseña (password) que se validan en el servidor de seguridad, donde el login identifica la persona dentro de la red y el password es la clave que le permite al usuario el acceso. Se deberá seleccionar un buen password y mantenerlo de forma confidencial. Considerando un buen password, todo "String" (conjunto de caracteres) que mantenga las siguientes características:
- Mínimo 6 caracteres (letras) en total al menos incluyendo dos números.
- El orden de inicialización del password, ya sea con caracteres o números es indiferente.
- El password es colocado por el usuario en su ingreso a la primera sesión de trabajo en la red y sistema operativo. El password de las aplicaciones será distinto al del sistema operativo y en primera instancia será proporcionado por el Jefe de seguridades; el usuario deberá cambiar el mismo en su primer ingreso a la utilización de la aplicación.

- El password de cada usuario caduca en 45 días, por lo cual el sistema operativo recordará al usuario la fecha de cambio de password de forma automática.
- Cada cuenta de usuario puede acceder a la red desde los equipos designados para su uso y a las computadoras dentro de su departamento.
- La cuenta de usuario (login) y contraseña (password) es personal e intransferible y no deben ser cedidos a terceros bajo ninguna circunstancia.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Los usuarios no deberán copiar a un medio removible (como un diskette), software, reportes o datos importantes de la Institución, sin la aprobación previa del Jefe Departamental.
- No pueden extraerse datos para ser utilizados fuera de la sede de la Institución sin la aprobación previa del Director del Área, ni utilizar otros recursos como computadoras portátiles o el servicio de Internet para extraer datos pertenecientes a la Institución.
- Se deberá implementar un procedimiento formal para la revisión periódica de los derechos de acceso y privilegios de los usuarios.
- Se deberán establecer documentaciones respectivas de los derechos y privilegios de los usuarios a los diferentes servicios, como por ejemplo uso de Internet y correo electrónico; dichos privilegios deberán ser autorizados por el Jefe Inmediato y Directores de Área respectivamente.
- Las conexiones remotas deberán ser identificadas y registradas correctamente.
- Todos los usuarios deben de tener un identificar único (ID del usuario) para su uso personal y exclusivo, de manera que se puedan rastrear las actividades de los usuarios.
- Los sistemas de administración de contraseña debe asegurar que el usuario final coloque una contraseña efectiva de acuerdo al nivel de seguridad esperado.
- Las terminales inactivas en lugares de alto riesgo o que sirvan a sistemas de alto riesgo se deben desactivar después de un periodo de inactividad, para impedir el acceso a ellas por parte de personas no autorizadas.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Se deberán aplicar restricciones en los tiempos de conexión de los usuarios, para brindar seguridad adicional en aplicaciones de alto riesgo.
- Se deberá restringir la información a los usuarios de acuerdo a sus funciones y responsabilidades dentro de la Institución. La asignación de opciones por medio de los sistemas serán estrictamente autorizadas por los respectivos jefes departamentales y Directores de Área.
- Los sistemas sensibles deberán tener entornos informáticos aislados.
- Se deberán generar registros de auditoria y se debe acordar un tiempo de uso adecuado, para ayudar a investigaciones futuras y seguimientos del control de acceso.
- Se deben establecer procedimientos para hacer seguimientos del uso de las instalaciones de procesamiento de la información, y se debe revisar regularmente el resultado del seguimiento de las actividades.
- Los relojes de computador se deben sincronizar para obtener un registro exacto.
- Las computadoras móviles o "laptos" deberán ingresar a la red y dominio de la Institución en el trabajo normal y diario en la misma, lo cual permitirá chequeo del equipo mediante el antivirus corporativo y controles de red de los equipos. Se les asignará clave particular para su ingreso fuera de la red de la institución manteniendo las políticas de chequeo y control de software malicioso.

POLÍTICAS PARA EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivos:

- Garantizar que la seguridad esté incorporada en los sistemas de información.
- Proteger la confidencialidad, autenticidad o integridad de la información.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Asegurar que los proyectos de Tecnología de Información (TI) y las actividades de soporte se lleven a cabo de una forma segura.
- Mantener la seguridad del software y la información de la aplicación del sistema.

Políticas:

- Los requisitos de la Institución en cuanto a los sistemas de información y aplicaciones, deben estar debidamente sustentados por el personal o usuarios solicitantes y legalizados por el Director del Área.
- Los sistemas de información y aplicaciones deberán tener los controles respectivos de validación para asegurar que los datos ingresados sean correctos y apropiados.
- Los controles de salidas de los datos deben ser validados para garantizar que el procesamiento de la información almacenada es correcto y apropiado.
- Se deberán desarrollar procedimientos de controles criptográficos para la protección de la información.
- Se debe utilizar cifrado para proteger la confidencialidad de la información sensible o crítica.
- Se deberán establecer procedimientos de control de calidad del software y de las aplicaciones antes de su salida a producción.
- Deben considerarse procedimientos para la implementación de software y verificaciones de compatibilidad en el sistema operativo.
- Los datos necesarios para las pruebas deben protegerse, controlarse y eliminarse una vez cumplido su correcto objetivo y utilización.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- El acceso a las librerías de los programas fuentes debe ser controlado y supervisado por el Jefe de Seguridad de la Institución.
- Deberán existir procedimientos formales de control de cambios con respecto a los sistemas de información; el procedimiento de control de cambios será de responsabilidad del Jefe de Desarrollo, mientras que la supervisión y el paso de los cambios de ambientes de desarrollo a producción será responsabilidad del Jefe de Seguridades.
- Las aplicaciones del sistema deben ser correctamente probadas y revisadas cuando se ejecuten los cambios.
- Los analistas programadores no podrán tener acceso a las librerías de los programas fuentes ni a los datos que se encuentran en producción.
- La aceptación de cambios y requerimientos ejecutados deberá formalizarse por medio de un procedimiento que contemple la aceptación del usuario por medio de un proceso manual o automatizado.
- La planeación de nuevos sistemas de información se realizará de forma conjunta con el área que realiza el requerimiento, y las especificaciones y alcances de los nuevos sistemas estarán documentadas y legalizadas en un acta formal de trabajo.
- En vista de que la Institución tiene terciarizado su proceso de desarrollo y mantenimiento de los sistemas, cualquier desacuerdo o incidentes en las etapas de desarrollo de software (análisis, diseño, desarrollo, implementación y mantenimiento) deberá ser informada de forma escrita a la empresa responsable de dicho proceso dentro de la Institución.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Los procedimientos de seguridad y controles con respecto a los sistemas de información deberán ser respectivamente comunicados y transmitidos al contratista responsable del proceso, así como cualquier actualización, modificación o cambio en las políticas de seguridad referentes a los sistemas y aplicaciones.

POLÍTICAS RESPECTO A LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivos:

- Contrarrestar las interrupciones a las actividades del negocio y proteger sus procesos de los efectos de fallas o desastres de gran magnitud.

Políticas:

- La institución deberá contar con un plan de contingencia y de continuidad del negocio debidamente aprobado por la máxima autoridad.
- El plan de continuidad del negocio y de recuperación ante desastres debe ser documentado y debidamente probado dentro de la organización.
- El plan de continuidad del negocio y de recuperación ante desastres deberán ser puestos a prueba regularmente y se deben llevar a cabo revisiones regulares para asegurar su actualización y eficacia.
- Las responsabilidades en estado crítico y pérdida de la continuidad del negocio deben encontrarse claramente detalladas y especificadas en dicho plan.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

POLÍTICAS DE CUMPLIMIENTO

Objetivos:

- Evitar incumplimiento a cualquier ley civil o penal, obligaciones estatutarias, reglamentarias o contractuales de cualquier requisito de seguridad.
- Asegurar el cumplimiento de los sistemas con las normas y políticas de seguridad organizacionales.
- Maximizar la eficacia del proceso de auditoria del sistema y minimizar la interferencia de éste.

Políticas:

- Todos los requisitos con respecto a la ley deben ser contemplados en todos y cada uno de los sistemas de información.
- Se prohíbe el uso de software no licenciado en los equipos informáticos de la Institución.
- Se deberán implementar procedimientos apropiados para asegurar el cumplimiento de las restricciones legales sobre el uso de material protegido por los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
- Los registros críticos e importantes a nivel institucional deben ser correctamente protegidos contra las pérdidas, destrucción y falsificación.
- Las respectivas direcciones deben autorizar el uso de las instalaciones de procesamiento de la información y evitar el mal uso de las mismas.

	POLÍTICA DE SEGURIDAD			
Institución:	H. Consejo Provincial del Guayas		Número:	001
Ubicación 1:	Centro: Malecón e Illingwoth esquina		Fecha:	02/01/2006
Ubicación 2:	Plaza Dañin y Pedro Menéndez Gilberth		Número de Páginas:	
Teléfonos:	2511677-676 2293268 2286158	Emitido en (Departamento):	Coordinación de Informática	

- Los directores deben establecer y emprender acciones para asegurar que todos los procedimientos de seguridad dentro de su área se lleven a cabo correctamente, y que todas las áreas dentro de la organización están sujetas a revisión regular, para revisar el cumplimiento de las políticas y normas de seguridad.
- Se deberán ejecutar procedimientos de revisión y control para verificar que todos los sistemas de información estén cumplimiento con los requisitos y normas legales.
- Las auditorias que se realicen al área de sistemas deberán ser planificadas y acordadas cuidadosamente, de tal forma que no afecte o interrumpa a los procesos normales del negocio.

Aprobada por:

PREFECTO PROVINCIAL

COORDINADOR DE INFORMÁTICA

Fecha de última revisión:	31 de Enero del 2006.

GESTIÓN DE RIESGOS

EVALUACIÓN DE OBJETIVOS DE CONTROL ISO 17799:2000

INTRODUCCIÓN.-

Con los resultados proporcionados del Análisis de Riesgo, se determinó el alcance de nuestro proyecto de tesis "Diseño de un Sistema de Gestión de seguridad informática", centrándose en la evaluación de los siguientes dominios cuyos Objetivos de control presentaron un nivel de riesgo alto.

DOMINIO	Objetivos de Control
Política de Seguridad	Política de Seguridad de Información.
Organización de la Seguridad	Seguridad del acceso de terceras personas.
Seguridad Física y Ambiental	Áreas de seguridad
	Seguridad del equipo
	Controles Generales
Control de Accesos	Administración de accesos de usuarios
	Responsabilidades del usuario
	Control de acceso al sistema operativo

Para un mejor entendimiento a continuación se detallará una breve descripción de los Objetivos de Control seleccionados:

3. Política de Seguridad

3.1 Política de seguridad de la información .-

- **Objetivo: Proporcionar dirección y apoyo gerencial para brindar seguridad de la información. El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.**

4. Organización de la Seguridad

4.2 Seguridad frente al acceso por parte de tercero.-

- Objetivo: **Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.**

El acceso a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado.

Cuando existe una necesidad de la empresa para permitir dicho acceso, debe llevarse a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control. Los controles deben ser acordados y definidos en un contrato con la tercera parte.

El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso. Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información.

7. Seguridad Física y Ambiental

7.1 Áreas seguras.-

- Objetivo: **Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.**

  Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

La protección provista debe ser proporcional a los riesgos identificados. Se recomienda la implementación políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de información.

7.2 Seguridad del equipo.-

- Objetivo: **Impedir pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.**

  El equipamiento debe estar físicamente protegido de las amenazas a la seguridad y los peligros del entorno.

  Es necesaria la protección del equipamiento (incluyendo el que se utiliza en forma externa) para reducir el riesgo de acceso no autorizado a los datos y para prevenir pérdidas o daños. Esto también debe tener en cuenta la ubicación y disposición equipamiento. Pueden requerirse controles especiales para prevenir peligros o accesos no autorizados, y para proteger instalaciones de soporte, como la infraestructura de cableado y suministro de energía eléctrica.

7.3 Controles generales.-

- Objetivo : **Impedir la exposición al riesgo o robo de la información o de las instalaciones de procesamiento de la misma.**

  Las instalaciones de procesamiento de la información y la información deben ser protegidas contra la divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños.

9. Control de Accesos

9.2 Administración de accesos de usuarios.-

- Objeto: Impedir el acceso no autorizado en los sistemas de información.

  Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.

  Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso de privilegio, que permiten a los usuarios pasar por alto los controles de sistema.

9.3 Responsabilidades del usuario .-

- Objeto: **Impedir el acceso usuarios no autorizados.**

  La cooperación de los usuarios autorizados en esencial para la eficacia de la seguridad.

  Se debe concienciar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

9.5 Control de acceso al sistema operativo.-

- Objetivo: **Impedir el acceso no autorizado al computador**

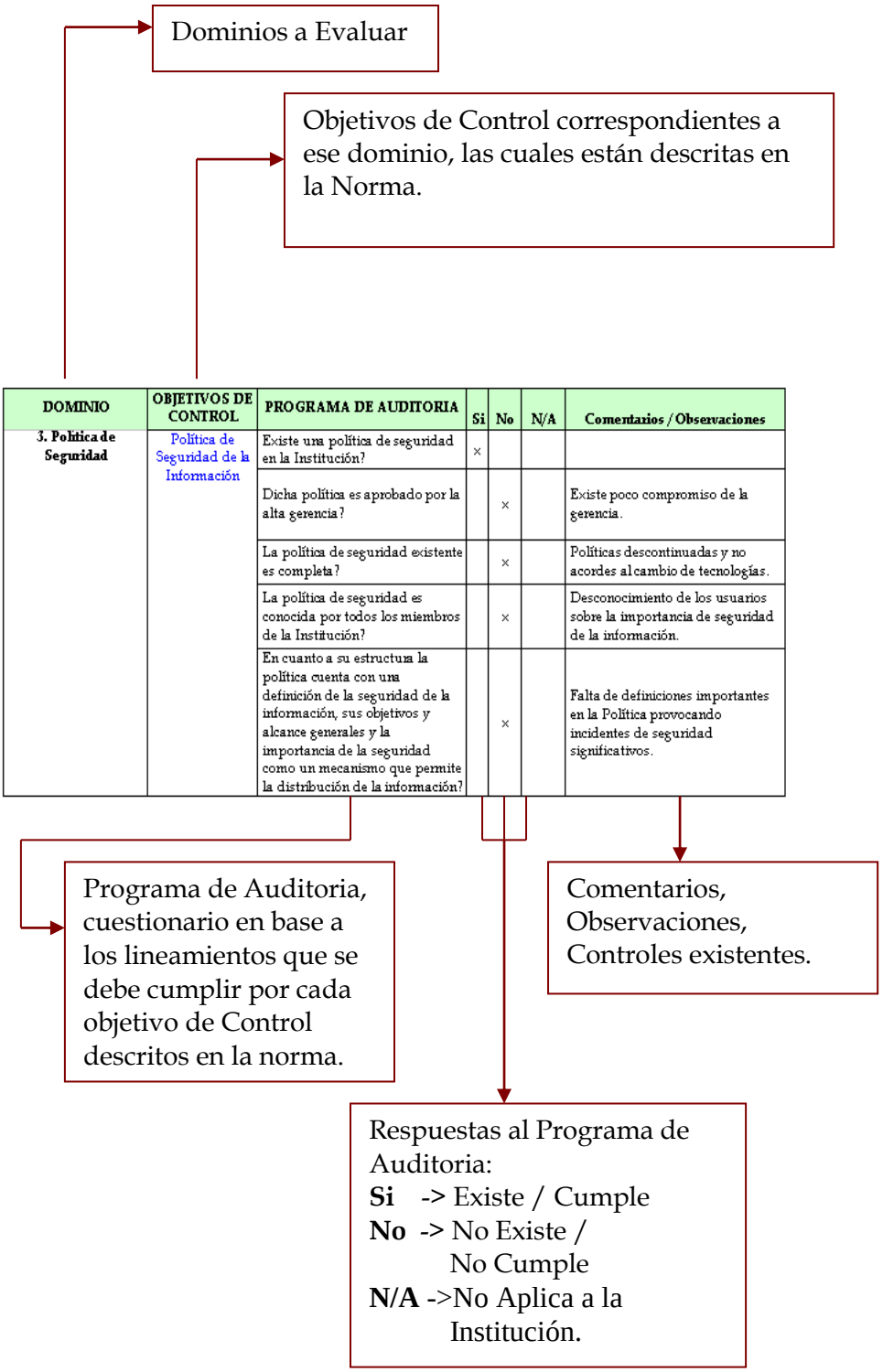
  Los mecanismos de seguridad a nivel del sistema operativo deben ser utilizados para restringir el acceso a los recursos del computador. Estas facilidades deben tener la capacidad de llevar a cabo lo siguiente:

  a) identificar y verificar la identidad y, si fuera necesario, la terminal o ubicación de cada usuario autorizado ;
  b) registrar los accesos exitosos y fallidos al sistema ;
  c) suministrar medios de autenticación apropiados; si se utiliza un sistema de administración de contraseñas, éste debe asegurar la calidad de las mismas ;
  d) restringir los tiempos de conexión de los usuarios, según corresponda.

  Se debe disponer de otros métodos de control de acceso, como "challenge-response", si están justificados por el riesgo comercial

EXPLICACIÓN DE LA METODOLOGÍA.-

Para una mejor comprensión en la documentación se utilizó el siguiente cuadro para la evaluación de los Objetivos de Control:



DOMINIO	OBJETIVOS DE CONTROL	PROGRAMA DE AUDITORIA	Si	No	N/A	Comentarios / Observaciones
3. Politica de Seguridad	Política de Seguridad de la Información	Existe una política de seguridad en la Institución?	×			
		Dicha política es aprobado por la alta gerencia?		×		Existe poco compromiso de la gerencia.
		La política de seguridad existente es completa?		×		Políticas descontinuadas y no acordes al cambio de tecnologías.
		La política de seguridad es conocida por todos los miembros de la Institución?		×		Desconocimiento de los usuarios sobre la importancia de seguridad de la información.
		En cuanto a su estructura la política cuenta con una definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo que permite la distribución de la información?		×		Falta de definiciones importantes en la Política provocando incidentes de seguridad significativos.

DESARROLLO

EVALUACIÓN DE OBJETIVOS DE CONTROL ISO 17799:2000

EVALUACIÓN DE OBJETIVOS DE CONTROL ISO 17799

DOMINIO	OBJETIVOS DE CONTROL	PROGRAMA DE AUDITORIA	Si	No	N/A	Comentarios / Observaciones
3. Política de Seguridad	Política de Seguridad de la Información	Existe una política de seguridad en la Institución?	x			
		Dicha política es aprobado por la alta gerencia?		x		Existe poco compromiso de la gerencia.
		La política de seguridad existente es completa?		x		Políticas descontinuadas y no acordes al cambio de tecnologías.
		La política de seguridad es conocida por todos los miembros de la Institución?		x		Desconocimiento de los usuarios sobre la importancia de seguridad de la información.
		En cuanto a su estructura la política cuenta con una definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo que permite la distribución de la información?		x		Falta de definiciones importantes en la Política provocando incidentes de seguridad significativos.

		La política presenta una adecuada declaración del propósito de los responsables del nivel gerencial, apoyando los objetivos y principios de la seguridad de la información?		x		Falta de apoyo al área de seguridad de la información
		La política presenta una breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad?		x		Indicios de nuevas vulnerabilidades o cambios en la infraestructura técnica o de la organización
		La Política cuenta con una adecuada definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información?		x		Falta de un compromiso por escrito por parte de las áreas responsables en las políticas establecidas.
		La Política cuenta con referencias a documentos que puedan respaldar lo escrito?	x			Observamos Boletines de Seguridad. Políticas publicadas en la Intranet.
		Existen procedimientos de revisión y evaluación?	x			
		La política de seguridad de la institución cuenta con un propietario que sea el responsable de su mantenimiento y revisión?		x		Falta de apoyo al área de seguridad de la información

		La institución cuenta con un control de revisiones periódicas sobre la eficacia de la política, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados?		x		Políticas descontinuadas y no acordes al cambio de tecnologías.
		La institución cuenta con un control de revisiones periódicas sobre el costo e impacto de los controles en la eficiencia del negocio?		x		
		La institución cuenta con un control de revisiones periódicas sobre los efectos de los cambios en la tecnología?		x		

DOMINIO	OBJETIVOS DE CONTROL	PROGRAMA DE AUDITORIA	Si	No	N/A	Comentarios / Observaciones
4. ORGANIZACIÓN DE LA SEGURIDAD	Seguridad del acceso de terceras personas	Existen procesos del área IT tercializados?	x			
		El acceso a terceras personas es limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible?		x		Accesos físicos no autorizados de terceras personas, la razón es por la mala división de los departamentos; como ejemplo se observó que el área de desarrollo de sistemas está ubicado en la dirección de la coordinación ejecutiva y en el mismo piso se encuentra la dirección de recursos humanos y por ende existe muchas visitas externas; y el área de Telecomunicaciones (Closet) se encuentra en la dirección de obras públicas.
		Se lleva un control de entrada por medio de tarjetas magnéticas o por otro medio electrónico o alguna identificación del acceso de terceras personas?	x			Existe control de tarjetas magnéticas asignadas a terceras personas.

		Se lleva un control de entrada por medio de tarjetas magnéticas o por otro medio electrónico o alguna identificación del acceso del personal tercializado?	x			Existe control de tarjetas magnéticas asignadas al personal tercializado.
		Se lleva un adecuado control en cuanto a los accesos lógicos, por Ej. a las bases de datos y sistemas de información de la organización de las terceras personas?		x		Accesos lógicos no autorizados de terceras personas, se observó que tienen acceso a las bases de datos pero están supervisados por una persona de la institución.
		La institución cuenta con una política de seguridad de terceras personas?		x		
		Existen definición de niveles de seguridad definidos formalmente en contratos con terceros?		x		La Institución cuenta con procesos del área IT tercializados en los cuales no se han definido en sus contratos los niveles de seguridad correctos.
		Los contratos a las terceras personas se encuentran bien definidos en cuanto a sus niveles de servicios a ofrecer, confidencialidad de la información?		x		Se debe reestructurar los contratos a terceras personas y en ellos se debe contemplar una cláusula de confidencialidad de la información a la cual ellos van a tener acceso; para evitar el robo y manipulación de los mismos.

DOMINIO	OBJETIVOS DE CONTROL	PROGRAMA DE AUDITORIA	Si	No	N/A	Comentarios / Observaciones
7. SEGURIDAD FISICA Y AMBIENTAL	Áreas de seguridad	El perímetro de seguridad está claramente definido?	x			
		El perímetro del edificio o área que contiene las instalaciones de procesamiento de información es físicamente sólido?		x		Ventanales grandes en el área de servidores, en caso de algún desastre natural, puede ocasionar accidentes o accesos no autorizados de personas.
		Existe un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio?	x			Existe control de ingreso por medios magnéticos y cámaras de seguridad
		El acceso a las distintas áreas y edificios está restringido exclusivamente al personal autorizado?	x			
		Existe un mecanismo de apagado automático de todo el centro de computo?		x		En caso de desastres naturales especialmente los incendios; sin el mecanismo apagado automático ocasionaría más pérdidas materiales a la institución.
		Cuando llegan visitantes a las áreas protegidas, son supervisados o inspeccionados y a la vez se lleva un registro con la fecha y horario de su ingreso y egreso?	x			Existe el control de tarjetas magnéticas asignadas al personal visitante mediante registro de cédulas

		Se lleva un control de entrada por medio de tarjetas magnéticas o por otro medio electrónico o alguna identificación laboral?	x			Existe control de tarjetas magnéticas asignadas al personal laboral.
		Las puertas y ventanas se bloquean cuando no hay vigilancia?	x			Existen controles de accesos físicos.
		Son controlados y limitados exclusivamente a las personas autorizadas el acceso a la información sensible, y a las instalaciones de procesamiento de información?		x		Accesos no autorizados a áreas de mayor cuidado.
		Las instalaciones clave están ubicadas en lugares a los cuales no pueda acceder el público?		x		
		En el centro de computo, sus instalaciones son discretas y poseen un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información?		x		

		Las funciones y el equipamiento de soporte, por Ej. Fotocopiadoras, máquinas de fax, están ubicados adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información?		x		
		Existe un guardia de seguridad en las áreas de procesamiento de información?		x		No hay una persona que controle las entradas y salidas de personas no autorizadas en las áreas de mayor cuidado como es el centro de cómputo ya que se encuentra ubicada en áreas de mayor presencia de visitantes externos.
		La dirección de sistemas se encuentra aislada de los demás departamentos.		x		Se observó que el área de desarrollo de sistemas está ubicado en la dirección de la coordinación ejecutiva y en el mismo piso se encuentra la dirección de recursos humanos y por ende existe muchas visitas externas; y el área de Telecomunicaciones se encuentra en la dirección de obras públicas.
		Tienen implementado adecuados sistemas de detección de intrusos? (Los mismos deben ser instalados según estándares profesionales y probados periódicamente.)		x		Daños e intrusiones

		Se encuentran las instalaciones de procesamiento de información administradas por la organización físicamente separadas de aquellas administradas por terceros?		x		
		Las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible no deben ser fácilmente accesibles al público. Se cumple este control?	x			
		Los materiales peligrosos o combustibles se encuentran almacenados en lugares seguros a una distancia prudencial del área protegida?		x		El almacenamiento del material combustible de la planta generadora de energía se encuentra ubicado en la terraza del edificio.
		Las áreas protegidas desocupadas se encuentran físicamente bloqueadas y periódicamente son inspeccionadas?	x			Controles de accesos físicos.
		El personal del servicio de soporte externo tienen acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible?	x			

	Seguridad de los equipos	Se lleva un control de acceso a las áreas de computo, desde el exterior de la sede de la organización? (limitado a personal que sea previamente identificado y autorizado).	x			
		Se lleva un control sobre el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información?		x		Robo, pérdida y modificación de la información y activos.
		Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, se encuentran ubicados en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso?		x		Daños de equipos por ubicación: Incendio, robos, vibraciones, polvo, humo, agua y comidas y bebidas.
		La organización cuenta con una política respecto de comer, beber y fumar cerca de las instalaciones de procesamiento de información?	x			

		La institución lleva un control de monitoreo sobre las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información?		x		
		Se debe considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ej. un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle. La institución posee este control?		x		Daños de equipos o pérdida de integridad de la información por factores externos.
		La sala de computo cuenta con una arquitectura idónea de suministros de energía?	x			Controles de suministros de energía y mecanismos alternos para evitar los cortos imprevistos.
		Cuentan con un generador de respaldo (planta de energía) para asegurar la continuidad del suministro de energía?	x			

		Los equipos principales cuentan con la ayuda de UPS?, en caso de apagones de luz?	x			
		Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información tienen una adecuada protección alternativa?	x			
		Los cables de energía se encuentran separados de los cables de comunicaciones? (con el fin de evitar interferencias)	x			
		Los interruptores de emergencia se encuentran ubicados cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento? (con el fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica)		x		En caso de desastres naturales especialmente los incendios; sin ese mecanismo ocasionaría más perdidas materiales a la institución.
		Se lleva una adecuada protección en el cableado de red contra interceptación no autorizada o daño?.		x		Interferencias, daños e intrusos.

		Existe un debido acuerdo sobre los niveles de servicios que ofrecen los proveedores en el mantenimiento de los equipos?	x			Contratos bien definidos.
		Se lleva un control sobre las reparaciones y mantenimientos de los equipos?	x			Controles de mantenimiento de equipo e historial de reparaciones de equipos por departamento.
		Cuentan con una bitácora histórica de registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo?	x			
		Se lleva un control de entradas y salidas de los equipos?	x			Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.
		Los equipos que posee la institución son asegurados?	x			Procedimiento de registros de seguros de equipos y compromisos con la empresa aseguradora.
		Los equipos que proveen los proveedores tienen garantías?	x			Procedimiento de adquisición de equipos a los proveedores.

	Controles Generales	Existe una política sobre la confidencialidad de los documentos en papel y medios informáticos por parte del personal, para cuando estos no se encuentren en uso y sean guardados en un mobiliario seguro bajo llave o en su respectivo archivero donde lo saco?		x		Robo, pérdida y modificación de la información y activos.
		Existe una política de seguridad de la información, la cuál indique al personal que debe apagar las computadoras personales, terminales e impresoras o colocar una adecuada cerradura de seguridad, contraseñas u otros controles cuando no se encuentren en uso?		x		
		Se lleva un control sobre puntos de recepción y envío de correo y las máquinas de fax y teléx no atendidas?		x		
		Tienen un control los empleados en el uso de las fotocopiadoras?		x		

		Existe un control sobre las autorizaciones de retiros de información o software de la sede de la organización?	x			Procedimiento de solicitud por escrito con firmas de responsables de cada dueño de la información por área.
		Se lleva a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la organización?	x			Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.
		El personal tiene conocimiento de la realización de dichas comprobaciones?	x			

DOMINIO	OBJETIVOS DE CONTROL	PROGRAMA DE AUDITORIA	Si	No	N/A	Comentarios / Observaciones
9. CONTROL DE ACCESOS	Administración de accesos de usuarios	Existe un procedimiento formal de registros de altas y bajas de usuarios a los sistemas de información.	x			Solicitudes de acceso a la red, solicitudes de acceso a los sistemas
		Se administra los privilegios de acceso a los usuarios para impedir accesos no autorizados.	x			El administrador de la red realiza la definición de políticas en servidor de dominio por usuarios y grupos de usuarios
		Existe un procedimiento formal para la administración de asignación de contraseñas a usuarios		x		Desconocimiento de los usuarios sobre la responsabilidad de las contraseñas en la empresa
		Existe un proceso formal de revisión de los controles de accesos a datos y servicios de TI y a intervalos regulares.		x		Asignación de accesos a usuarios sin firmas de responsabilidad o autorización
	Responsabilidades del usuario	Los usuarios siguen buenas prácticas de seguridad en la selección y uso de contraseñas.		x		Divulgación de contraseñas, fáciles de identificar, contraseñas iguales para varios usuarios
		Garantizan los usuarios la seguridad de sus equipos desatendidos durante un periodo extenso por los usuarios, mediante notificaciones sobre puntos a cumplir		x		Accesos no autorizados a equipos e información

	Control de acceso al sistema operativo	Existen controles para identificar automáticamente los terminales que inician sesión en el sistema.	x			Logs del sistema operativo, reportes de módulo de seguridad de acceso de usuarios a las aplicaciones
		Existen procedimientos de control de conexión de terminales para minimizar la oportunidad de acceso no autorizado.		x		Accesos no autorizados debido a la facilidad del sistema o de los mensajes mostrados.
	Control de acceso al sistema operativo	Todos los usuarios poseen un identificador único y exclusivo de acceso y autenticación, de modo que se puedan establecer responsabilidades de las actividades realizadas y que puedan ser rastreadas.	x			Se han establecido claves de identificación para cada uno de los usuarios que tienen acceso a los sistemas de información.
		Existen algún sistema de administración de contraseñas que garantice contraseñas de calidad		x		Contraseñas poco confiables y fácilmente descifrables
		Está controlado el uso de utilitarios de sistemas para evitar que pasen por alto los controles se sistemas y aplicaciones.	x			Existen restricciones para cada equipo, para que solo se ejecuten las aplicaciones necesarias apara sus labores diarias.
		Existen alarmas silenciosas como medio de protección a usuarios.		x		Accesos no autorizados bajo presiones de personal mal intencionado.

		Las terminales inactivas en ubicaciones de riesgo se apagan después de un periodo de inactividad para evitar acceso de personas no autorizados.	x			Se realiza un control manual de las terminales con un tiempo de inactividad grande.
		Existe un límite de horario de conexión para brindar seguridad adicional en aplicaciones sensibles o de alto riesgo.	x			Los límites están dispuesto 1 hora antes y una hora después del horario dependiendo de cada usuario.

EVALUACIÓN DE CONTROLES EXISTENTES

INTRODUCCIÓN .-

Luego de la Evaluación de los Objetivos de Control de los dominios seleccionados, nuestra siguiente tarea fue una verificación del diseño e implantación de los controles existentes en el Honorable Consejo Provincial del Guayas. Para ello, se procedió a revisar sucesivamente y en este orden el diseño y la implementación de los mismos:

Diseño: Si el control existe, se encuentra documentado, si es una política, proceso, norma o una práctica conocida y realizada.

Implementación: Si el control está funcionando de acuerdo al diseño; es decir si cumple con las políticas, normas, proceso o práctica establecida.

3. Política de Seguridad

- Boletines de Seguridad.
- Políticas publicadas en la Intranet.

4. Organización de la Seguridad

- Control de tarjetas magnéticas asignadas a Terceras personas.
- Control de tarjetas magnéticas asignadas a personal terciarizada.

7. Seguridad Física y Ambiental

- Control de cámaras de seguridad
- Tarjetas magnéticas asignadas al personal visitante mediante registro de cédulas.
- Tarjetas magnéticas asignadas al personal fijo.
- Controles de accesos físicos (Las puertas y ventanas se bloquean cuando no hay vigilancia).
- Controles de suministros de energía y mecanismos alternos para evitar los cortos imprevistos.

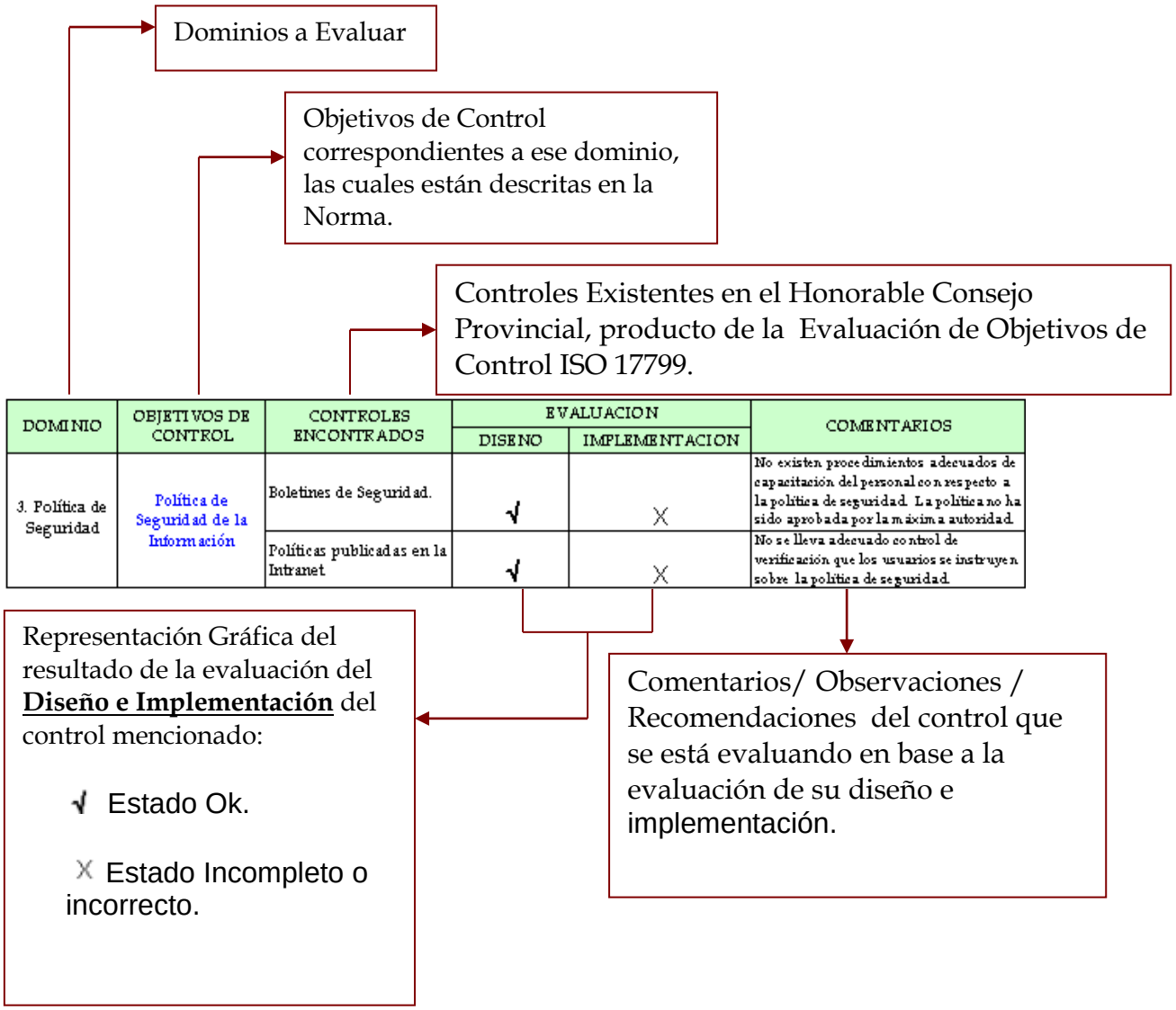
- Existe un debido acuerdo sobre los niveles de servicios que ofrecen los proveedores en el mantenimiento de los equipos y se encuentran detallados en los contratos (Contratos bien definidos).
- Controles de mantenimiento de equipo e historial de reparaciones de equipos por departamento.
- Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.
- Procedimiento de registros de seguros de equipos y compromisos con la empresa aseguradora.
- Procedimiento de adquisición de equipos a los proveedores.
- Procedimiento de solicitud por escrito sobre las autorizaciones de retiros de información o software de la sede de la organización con firmas de responsables de cada dueño de la información por área.

9. Control de Accesos

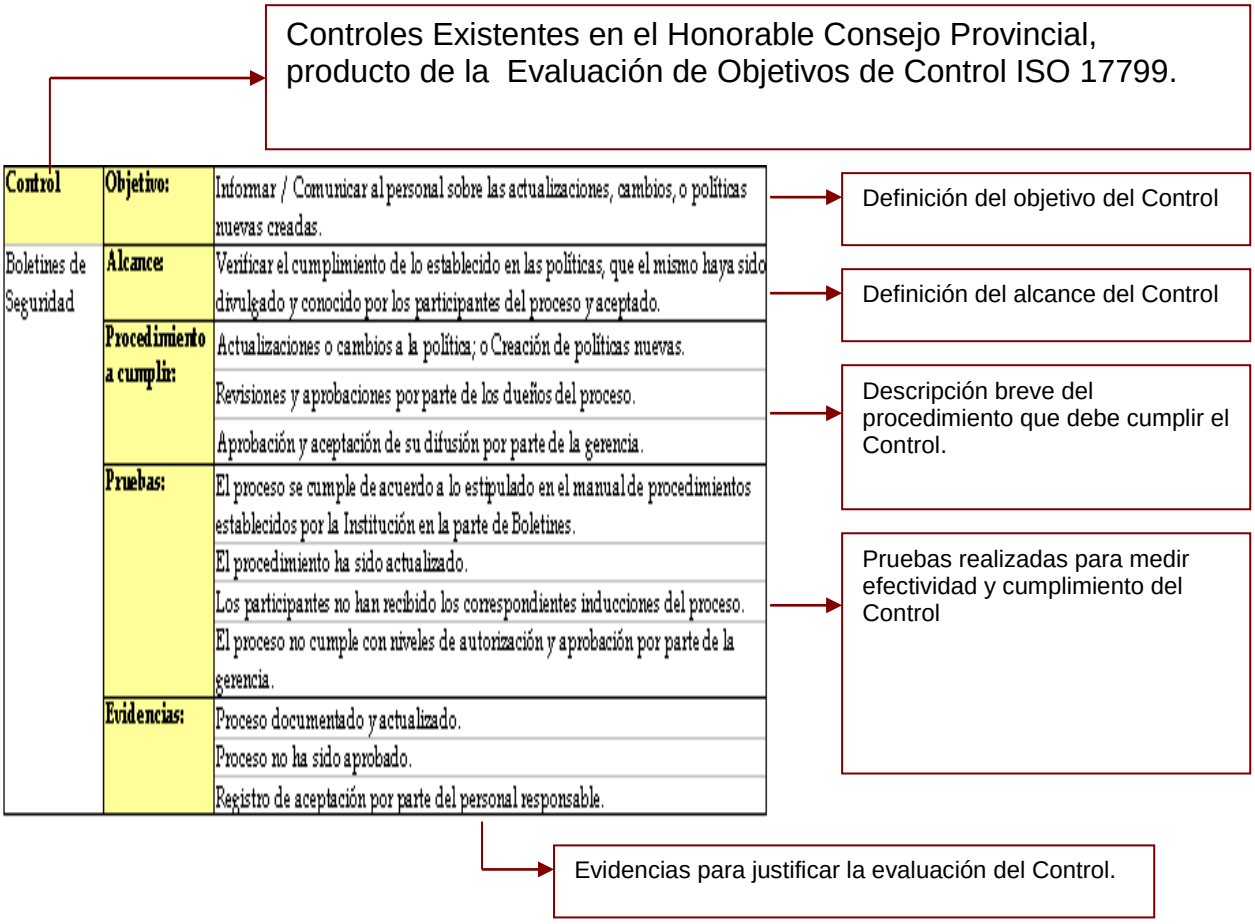
- Solicitudes de acceso a la red, solicitudes de acceso a los sistemas.
- El administrador de la red realiza la definición de políticas en servidor de dominio por usuarios y grupos de usuarios
- Logs del sistema operativo, reportes de módulo de seguridad de acceso de usuarios a las aplicaciones
- Se han establecido claves de identificación para cada uno de los usuarios que tienen acceso a los sistemas de información.
- Existen restricciones para cada equipo, para que solo se ejecuten las aplicaciones necesarias para sus labores diarias.
- Se realiza un control manual de las terminales con un tiempo de inactividad grande.
- Los límites están dispuesto 1 hora antes y una hora después del horario dependiendo de cada usuario.

EXPLICACIÓN DE LA METODOLOGÍA.-

Para un mejor entendimiento en la documentación se utilizó los siguientes cuadros para la evaluación de los controles:



Para un análisis más profundo de los controles se estructuró el siguiente cuadro de apoyo:



Control	Objetivo:	Informar / Comunicar al personal sobre las actualizaciones, cambios, o políticas nuevas creadas.
Boletines de Seguridad	Alcance:	Verificar el cumplimiento de lo establecido en las políticas, que el mismo haya sido divulgado y conocido por los participantes del proceso y aceptado.
	Procedimiento a cumplir:	Actualizaciones o cambios a la política; o Creación de políticas nuevas.
		Revisiones y aprobaciones por parte de los dueños del proceso.
		Aprobación y aceptación de su difusión por parte de la gerencia.
	Pruebas:	El proceso se cumple de acuerdo a lo estipulado en el manual de procedimientos establecidos por la Institución en la parte de Boletines.
		El procedimiento ha sido actualizado.
		Los participantes no han recibido los correspondientes inducciones del proceso.
		El proceso no cumple con niveles de autorización y aprobación por parte de la gerencia.
	Evidencias:	Proceso documentado y actualizado.
		Proceso no ha sido aprobado.
		Registro de aceptación por parte del personal responsable.

DESARROLLO:

EVALUACIÓN DE CONTROLES EXISTENTES DE LOS DOMINIOS EVALUADOS.

EVALUACIÓN DE CONTROLES EXISTENTES

DOMINIO	OBJETIVOS DE CONTROL	CONTROLES ENCONTRADOS	EVALUACION		COMENTARIOS
			DISEÑO	IMPLEMENTACION	
3. Política de Seguridad	Política de Seguridad de la Información	Boletines de Seguridad.	√	X	No existen procedimientos adecuados de capacitación del personal con respecto a la política de seguridad. La política no ha sido aprobada por la máxima autoridad.
		Políticas publicadas en la Intranet.	√	X	No se lleva adecuado control de verificación que los usuarios se instruyen sobre la política de seguridad.

Control	**Objetivo:**	Informar / Comunicar al personal sobre las actualizaciones, cambios, o políticas nuevas creadas.
Boletines de Seguridad	**Alcance:**	Verificar el cumplimiento de lo establecido en las políticas, que el mismo haya sido divulgado y conocido por los participantes del proceso y aceptado.
	Procedimiento a cumplir:	Actualizaciones o cambios a la política; o Creación de políticas nuevas. Revisiones y aprobaciones por parte de los dueños del proceso. Aprobación y aceptación de su difusión por parte de la gerencia.
	Pruebas:	El proceso se cumple de acuerdo a lo estipulado en el manual de procedimientos establecidos por la Institución en la parte de Boletines. El procedimiento ha sido actualizado. Los participantes no han recibido los correspondientes inducciones del proceso. El proceso no cumple con niveles de autorización y aprobación por parte de la gerencia.
	Evidencias:	Proceso documentado y actualizado. Proceso no ha sido aprobado. Registro de aceptación por parte del personal responsable.

Control	**Objetivo:**	Informar / Comunicar al personal sobre las actualizaciones, cambios, o políticas nuevas creadas que son publicadas en la intranet.
Políticas publicadas en la Intranet	**Alcance:**	Verificar el cumplimiento de lo establecido en las políticas, que el mismo haya sido leído y conocido en la intranet por los participantes del proceso y todo el personal autorizado a leerlo.
	Procedimiento a cumplir:	Actualizaciones o cambios a la política; o Creación de políticas nuevas en las páginas Web relacionadas. Revisiones y aprobaciones del diseño y contenido por parte de los dueños del proceso. Aprobación y aceptación de su publicación en la intranet por parte de la gerencia.
	Pruebas:	El proceso se cumple de acuerdo a lo estipulado en el manual de procedimientos establecidos por la Institución en la parte de Políticas publicadas en la Intranet. El procedimiento ha sido actualizado. Los participantes no han recibido los correspondientes inducciones del proceso. El proceso no cumple con niveles de autorización y aprobación por parte de la gerencia. El proceso se cumple con la parte de diseño y seguridades en el desarrollo de sus páginas web.
	Evidencias:	Bitácora de Auditoria de aceptación y aprobación de la política publicada en la intranet. Bitácora de Auditoria de entradas y salidas de los usuarios que han dedicado un poco de su tiempo en informarse sobre las políticas que existe en la institución. Registros de Accesos de personal autorizado para la lectura de las mismas.

DOMINIO	OBJETIVOS DE CONTROL	CONTROLES ENCONTRADOS	EVALUACION		COMENTARIOS
			DISEÑO	IMPLEMENTACION	
4. Organización de la Seguridad	Seguridad del acceso de terceras personas	Control de tarjetas magnéticas asignadas a Terceras personas.	√	X	Utilizan tarjetas magnéticas quemadas por piso, pero por la mala distribución de los departamentos esos visitantes tienen acceso a áreas sensibles como es el centro de computo.
		Control de tarjetas magnéticas asignadas a personal tercializada.	√	X	Utilizan tarjetas magnéticas que cumplen con el procedimiento de creación de tarjetas temporales, pero le falta identificación visual como es la foto, número de cédula y empresa a la cuál esta trabajando.

Control	**Objetivo:**	Comprobar la utilización del control y su cumplimiento.
Tarjetas magnéticas asignadas a Terceras Personas.	**Alcance:**	Verificar las autorizaciones correspondientes a las tarjetas magnéticas de acceso a las instalaciones de acuerdo al procedimiento establecido.
	Procedimiento a cumplir:	El visitante debe entregar la cédula en recepción. El personal de recepción verifica los datos por medio de su cédula en el padrón electoral. Luego hace la respectiva llamada de comprobación a la persona a quien esta buscando, para aprobar su ingreso. Entrega de las tarjetas magnéticas al visitante. (Tarjetas quemadas por piso).
	Pruebas:	Se comprobó las autorizaciones de las tarjetas que en realidad estén quemadas por piso. Se comprobó la existencia de un sistema de comprobación de cédula en el padrón electoral. Se entrevisto al personal de recepción y se observó el proceso de atención y entrega de tarjetas a los visitantes.
	Evidencias:	Registro de entradas y salidas del personal visitante. Registro de revisiones de comprobación de cédulas de identidad.

Control	**Objetivo:**	Comprobar la utilización del control, su cumplimiento y las autorizaciones del personal tercializado.
Tarjetas magnéticas asignadas a personal tercializada.	**Alcance:**	Verificar las autorizaciones correspondientes a las tarjetas magnéticas de acceso a las instalaciones de acuerdo al procedimiento establecido.
	Procedimiento a cumplir:	Listado de Personas Tercializadas activas en roles por parte del departamento de Recursos humanos. RRHH pasa a seguridad mantenimiento del edificio para que le asignen tarjetas temporales. Activación de las tarjetas con autorizaciones de entrada y salida a los departamentos autorizados. Entrega de la tarjeta a su propietario correspondiente, con la debida firma de recibido.
	Pruebas:	Se tomó una muestra de 50 personas que se encuentran Tercializadas, y se comprobó que estos tengan sus debidos accesos y en caso de encontrar personal que este inactivo que sus tarjetas hayan sido bloqueadas, desactivadas o eliminadas. Se verificó que las tarjetas magnéticas internamente tienen un control la cuál te indican tu horario de entrada y salida, fuera de esos horarios la tarjeta magnética no funciona y no te permite el ingreso a ningún departamento. Se comprobó que las tarjetas magnéticas internamente tiene un control la cuál te indica a que departamentos tienes autorizado el ingreso. Se verificó la existencia de registros de tarjetas magnéticas de acceso eliminadas o bloqueadas por mal estado o robo de las mismas.

		Se verificó la existencia de registros de tarjetas magnéticas de acceso desactivadas por razones de Vacaciones u otro tipo de inconvenientes por parte del personal que labora en la institución.
	Evidencias:	Existencia de solicitudes aprobadas, negadas, eliminadas, bloqueadas o desactivadas de tarjetas magnéticas con sus respectiva glosa indicando las razones de cambio de sus estados y firmas de responsables. Existencia de registros de tarjetas magnéticas de accesos aprobadas. Existencia de registros de tarjetas magnéticas de acceso eliminadas o bloqueadas por mal estado o robo de las mismas. Existencia de registros de tarjetas magnéticas de acceso desactivadas por razones de Vacaciones u otro tipo de inconvenientes por parte del personal que labora en la institución.

DOMINIO	OBJETIVOS DE CONTROL	CONTROLES ENCONTRADOS	EVALUACION		COMENTARIOS
			DISEÑO	IMPLEMENTACION	
7. SEGURIDAD FISICA Y AMBIENTAL	Áreas de seguridad	Control de cámaras de seguridad	√	X	Falta de cámaras de seguridades en varios puntos estratégicos. Como por ejemplo en el área de Servidores, en el pasillo donde se encuentra el centro de computo.
		Tarjetas magnéticas asignadas al personal visitante mediante registro de cédulas	√	X	Se observó que el control de tarjetas esta bien diseñado, e incluso cumple con el horario de visitas a los departamentos, ya que se comprobó que una vez llegada las 5:00 p.m. Automáticamente dejan de funcionar y no tienen acceso a ningún lugar; pero falta capacitación a los encargados de recepción ya que dejan entrar a cualquier persona sin llamar previamente a la persona con los que tienen la cita para darles el respectivo permiso de ingreso.
		Tarjetas magnéticas asignadas al personal fijo.	√	√	OK

		Controles de accesos físicos (Las puertas y ventanas se bloquean cuando no hay vigilancia).	√	√	OK
	Seguridad de los equipos				Cuentan con UPS para cada computador personal pero algunos poseen baterías dañadas.
		Controles de suministros de energía y mecanismos alternos para evitar los cortos imprevistos.	√	X	La institución cuenta con una Planta generadora la cual es encendida los días Viernes como medio de mantención de la misma y como para probar su funcionamiento; pero provoca una descarga las cuales a futuro ocasionaría problemas en los equipos electrónicos.
		Existe un debido acuerdo sobre los niveles de servicios que ofrecen los proveedores en el mantenimiento de los equipos y se encuentran detallados en los contratos (Contratos bien definidos).	√	X	En los contratos del personal de mantenimiento no se encontró definiciones sobre cláusulas de confidencialidad de la información.
					No existe una adecuada evaluación de personal.

					El personal de seguridad debe realizar un adecuado chequeo al personal de mantenimiento antes y después de que terminan su trabajo en la institución.
					No se lleva un registro de entradas y salidas de las visitas del personal de mantenimiento a las áreas de mayor cuidado.
					La institución tiene como precaución, el designar a una persona para que lo acompañe hasta que termine su trabajo.
					Este procedimiento aplica al personal de mantenimiento de equipos de hardware e instalaciones eléctricas y el personal de cableado de bus y datos.
		Controles de mantenimiento de equipo e historial de reparaciones de equipos por departamento.	√	√	OK

		Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.	√	√	OK
		Procedimiento de registros de seguros de equipos y compromisos con la empresa aseguradora.	√	X	Aplica solo a la Área financiera, centros de computo y equipo nuevos. Este procedimiento debería aplicar a todas las áreas para contrarrestar problemas de robos y daños de los mismos como ha sido sustentado en el presente documento.
		Procedimiento de adquisición de equipos a los proveedores.	√	√	OK
	Controles Generales	Procedimiento de solicitud por escrito sobre las autorizaciones de retiros de información o software de la sede de la organización con firmas de responsables de cada dueño de la información por área.	√	√	OK

Control	**Objetivo:**	Comprobar la utilización del control, su cumplimiento y las autorizaciones a las mismas.
Tarjetas magnéticas asignadas al personal fijo.	**Alcance:**	Verificar las autorizaciones correspondientes a las tarjetas magnéticas de acceso a las instalaciones de acuerdo al procedimiento establecido.
	Procedimiento a cumplir:	Listado de Personas activas en roles por parte del departamento de Recursos humanos. RRHH pasa a seguridad mantenimiento del edificio para que le asigne tarjeta Activación de las tarjetas con autorizaciones de entrada y salida a los departamentos autorizados. Entrega de la tarjeta a su propietario correspondiente, con la debida firma de recibido.
	Pruebas:	Se tomó una muestra de 50 personas, y se comprobó que estos tengan sus debidos accesos y en caso de encontrar personal que este inactivo que sus tarjetas hayan sido bloqueadas, desactivadas o eliminadas. Se verificó que las tarjetas magnéticas internamente tienen un control la cuál te indican tu horario de entrada y salida, fuera de esos horarios la tarjeta magnética no funciona y no te permite el ingreso a ningún departamento.
		Se comprobó que las tarjetas magnéticas internamente tiene un control la cuál te indica a que departamentos tienes autorizado el ingreso.
		Se verificó la existencia de registros de tarjetas magnéticas de accesos aprobadas y negadas.

		Se verificó la existencia de registros de tarjetas magnéticas de acceso eliminadas o bloqueadas por mal estado o robo de las mismas. Se verificó la existencia de registros de tarjetas magnéticas de acceso desactivadas por razones de Vacaciones u otro tipo de inconvenientes por parte del personal que labora en la institución. Se verificó que las tarjetas magnéticas de acceso solo se encuentren activadas las de personal activo.
	Evidencias:	Existencia de solicitudes aprobadas, negadas, eliminadas, bloqueadas o desactivadas de tarjetas magnéticas con sus respectiva glosa indicando las razones de cambio de sus estados y firmas de responsables. Existencia de registros de tarjetas magnéticas de accesos aprobadas. Existencia de registros de tarjetas magnéticas de accesos reprobadas. Existencia de registros de tarjetas magnéticas de acceso eliminadas o bloqueadas por mal estado o robo de las mismas.
		Existencia de registros de tarjetas magnéticas de acceso desactivadas por razones de Vacaciones u otro tipo de inconvenientes por parte del personal que labora en la institución.

Control	**Objetivo:**	Comprobar la utilización del control y su cumplimiento.
Controles de accesos físicos (Las puertas y ventanas se bloquean cuando no hay vigilancia)	**Alcance:**	Verificar que se cumplan las configuraciones que realiza el personal de seguridades de acceso en el sistema Query de acuerdo al procedimiento establecido.
	Procedimiento a cumplir:	Se utiliza el Sistema Query, el personal de seguridad realiza las respectivas configuraciones y automáticamente las puerta de vidrio y de madera se cierran, se apagan las luces de todos los departamentos y los aires acondicionados.
	Pruebas:	Se observó que las puertas y ventanas se cierran automáticamente a la hora programada. Se observó que las luces y aires acondicionados de todos los departamentos automáticamente son apagados a la hora programada.
	Evidencias:	Existencia del Sistema Query. Existen registros de configuraciones diarias por parte del personal de seguridad. Videos de seguridad.

Control	**Objetivo:**	Verificar el correcto funcionamiento del proceso de acuerdo a lo establecido.
Controles de mantenimiento de equipo e historial de reparaciones de equipos por departamento.	**Alcance:**	Verificar que se cumplan el ingreso de los mantenimientos de hardware que se realizan en la institución en el Sistema de Hardware de acuerdo al procedimiento establecido.
	Procedimiento a cumplir:	Se utiliza el Sistema de Hardware, el asistente de mantenimiento realiza los respectivos ingresos de todos los mantenimientos realizados en la institución con su respectivo detalle (Fechas, horas, observaciones y responsables).
	Pruebas:	Entrevista al asistente de mantenimiento. Comprobación paso a paso de cómo se lleva el proceso de ingreso de reparaciones de equipos en el Sistema de Hardware. Se verificó la existencia de registros en el sistema con todo sus detalles de mantenimiento. Se verificó los registros de partes y piezas dañadas o cambiadas. Se verificó los registros de las observaciones de los usuarios. Se verificó los registros de autorizaciones debidas para proceder con la reparación de los mismos.
	Evidencias:	Solicitudes aprobadas y negadas con sus respectiva observación indicando las razones de la adquisición o reparación de los equipos con su debida firmas de responsables y autorizaciones.

		Registros de llamadas y registros mediante procedimiento establecido para los usuarios de solicitud de mantenimiento de sus equipos. Registros en el sistema con todo sus detalles de mantenimiento. Registros de partes y piezas dañadas o cambiadas. Registros de las observaciones de los usuarios. Registros de autorizaciones debidas para proceder con la reparación de los mismos.

Control	**Objetivo:**	Comprobar la utilización del control y su cumplimiento.
Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.	**Alcance:**	Verificar si cumple con el procedimiento de las autorizaciones correspondientes a las entradas y salidas de los equipos cuando salen de la institución.
	Procedimiento a cumplir:	Documento formal indicando las características del equipo y un breve detalle del estado del mismo. Firma de autorización por parte de la coordinación de la institución. Firma de autorización del director de área. Firma de autorización de salida por parte del responsable del control del edificio.
	Pruebas:	Entrevista con el responsable del control del edificio. Se verificó que se realiza una correcta inspección de los equipos que salen y entran a la institución. Se verificó la existencia de registros de entradas y salidas de los equipos con sus respectivas firmas de autorización.
	Evidencias:	Documentos formales con sus respectivas firmas de autorizaciones de las entradas y salidas de los equipos. Solicitudes formales por parte de los usuarios, con su debida descripción de las anomalías que presenta.

Control	**Objetivo:**	Comprobar la utilización del control y su cumplimiento.
Procedimiento de adquisición de equipos a los proveedores.	**Alcance:**	Verificar su cumple con el procedimiento de adquisición de equipos nuevos para la institución.
	Procedimiento a cumplir:	Cada área envía una solicitud con el detalle de equipos que desean adquirir e indican para quien será destinado; con su respectiva autorización del director del área. La dirección hace requerimientos a la dirección administrativa, la dirección administrativa lo envía a la coordinación informática para que evalúen lo solicitado y coloquen su estado aprobado. Luego de que esta aprobado por la coordinación de informática se lo ingresa en el sistema de ruteo y seguimiento de trámites. Y finalmente se solicita la autorización del coordinador.
	Pruebas:	El proceso se cumple de acuerdo a lo estipulado en el manual de procedimientos establecidos para la institución. El proceso ha sido aprobado por la alta gerencia. Los participantes han recibido las correspondientes inducciones del proceso. El proceso se cumple con niveles de autorización y aprobación en el sistema. Se comprobó la efectividad del procedimiento al momento de adquirir nuevos equipos para la institución.
	Evidencias:	Se verificó la existencia de solicitudes aprobadas y negadas de equipos nuevos por parte de las áreas con sus respectivas autorizaciones.
		Se encontraron registros en el sistema de ruteo y seguimiento de trámites de las solicitudes aprobadas por la dirección, departamento de administración y coordinación informática.

Control	**Objetivo:**	Comprobar la utilización del control y su cumplimiento.
Procedimiento de solicitud por escrito sobre las autorizaciones de retiros de información o software de la sede de la organización con firmas de responsables de cada dueño de la información por área.	**Alcance:**	Verificar si cumple con el procedimiento de las autorizaciones correspondientes de las entradas y salidas de la información o software de la sede de la organización.
	Procedimiento a cumplir:	Documento formal indicando responsables de su traslado, firmas de autorización y lugar donde va ser entregado. Firma de autorización por parte de la coordinación de la institución. Firma de autorización del director de área.
	Pruebas:	Entrevista con el responsable del control del edificio. Se verificó la existencia de documentos formales de entradas y salidas de la información o software con sus respectivas firmas de autorización y registros de solicitudes de información por parte de los departamentos solicitantes.
	Evidencias:	Se verificó la existencia de los documentos con sus respectivas firmas de autorizaciones de las entradas y salidas de la información y software. Se verificó la existencia de las solicitudes formales por parte de los departamentos, con su debida descripción del motivo de su uso, responsables y autorizaciones de sus respectivos jefes de áreas.

DOMINIO	OBJETIVOS DE CONTROL	CONTROLES ENCONTRADOS	EVALUACION		COMENTARIOS
			DISEÑO	IMPLEMENTACION	
9. CONTROL DE ACCESOS	Administración de accesos de usuarios	Solicitudes de acceso a la red, solicitudes de acceso a los sistemas	√	X	Se verificó que existe la solicitud formal de acceso tanto a los sistemas de información, a la red y al sistema operativo.
					La solicitud consta de los siguientes puntos: nombre del usuario, identificador único de usuario, firma de autorización del jefe del área y los niveles de acceso.
					Se realizó pruebas de que todos los usuarios que se encuentran creados tengan el soporte respectivo y se encontraron usuarios que no cumplían esta condición.

		El administrador de la red realiza la definición de políticas en servidor de dominio por usuarios y grupos de usuarios	√	√	Se verificó que este control funciona, ya que están definidas la políticas de acceso a los servidores de acuerdo al tipo de usuario o al área a que pertenece.
					Las pruebas consistieron en verificar los diferentes niveles de privilegios, tanto para el sistema operativo, bases de datos, red
					No se encontraron novedades de usuarios que se encuentren creados sin pertenecer a algún dominio o grupo de usuarios.
	Control de acceso al sistema operativo	Logs del sistema operativo, reportes de módulo de seguridad de acceso de usuarios a las aplicaciones	√	√	Están habilitados los logs de los sistemas operativos y bases de datos, para determinar ingresos, salidas y otras actividades de los usuarios.
					Las pruebas consistieron verificar los logs del sistema operativo sobre una cuenta creada para las pruebas.

		Se han establecido claves de identificación para cada uno de los usuarios que tienen acceso a los sistemas de información.	√	√	Todos los usuarios poseen un identificador único y una contraseña asignada para el acceso a los diferentes sistemas de información.
					Las pruebas realizadas consistieron en realizar observaciones al ingreso de los usuarios al sistema desde su computador.
					El Sistema Operativo no permite identificadores de usuarios duplicados.
	Control de acceso al sistema operativo	Existen restricciones para cada equipo, para que solo se ejecuten las aplicaciones necesarias para sus labores diarias.	√	√	Existe creadas políticas a nivel de servidor sonde se restringe las aplicaciones que no se necesitan ejecutar o que no son necesarias.
					Se realizó pruebas ingresando en varias computadoras e intentando cambiar configuraciones de red y del sistema operativo para intentar tener acceso a otros recursos.
					No se encontraron novedades al realizar las pruebas.

		Se realiza un control manual de las terminales con un tiempo de inactividad grande.	X	X	El control se lo hace manualmente al inicio de cada día, identificando que usuarios han dejado los terminales activos.
		Los límites están dispuesto 1 hora antes y una hora después del horario dependiendo de cada usuario.	√	√	A todos los usuarios se les asigna esta regla de accesos. Se realizó pruebas intentando ingresar al sistema después del horario normal de labores. No se encontraron novedades al realizar las pruebas.

Control	**Objetivo:**	Debe existir un procedimiento formal de registro y eliminación de usuarios para otorgar acceso a todos los sistemas y servicios de información multi-usuario
Solicitudes de acceso a la red, solicitudes de acceso a los sistemas	**Alcance:**	Verificar que los usuarios que tienen acceso a los servicios de información hallan sido autorizados y aprobados con una solicitud formal.
	Procedimiento a cumplir:	Jefe del área realiza la solicitud de accesos de acuerdo a la responsabilidad asignada. El Administrador de red recibe la solicitud firmada por el jefe del área. El Administrador de red realiza la asignación de un identificador únicos y de los perfiles de acceso de acuerdo a la solicitud. Entrega al usuario su identificador de acceso y las indicaciones para registro por primera vez de su contraseña.
	Pruebas:	Se verificó que existe la solicitud formal de acceso tanto a los sistemas de información, a la red y al sistema operativo.
		La solicitud consta de los siguientes puntos: nombre del usuario, identificador único de usuario, firma de autorización del jefe del área y los niveles de acceso.
		Se realizó pruebas de que todos los usuarios que se encuentran creados tengan el soporte respectivo y se encontraron usuarios que no cumplían esta condición.
	Evidencias:	Solicitudes firmadas y aprobadas, listas de usuarios registrados en la red.

Control	**Objetivo:**	Se debe limitar y controlar la asignación y uso de privilegios. Los sistemas multi-usuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.
El administrador de la red realiza la definición de políticas en servidor de dominio por usuarios y grupos de usuarios	**Alcance:**	Verificar que se realice una administración de privilegios que minimice el acceso de usuarios no autorizados.
	Procedimiento a cumplir:	El Administrador de la red configura los privilegios de los usuarios o grupos de usuarios de acuerdo al área o responsabilidad asignadas.
	Pruebas:	Se verificó que este control funciona, ya que están definidas la políticas de acceso a los servidores de acuerdo al tipo de usuario o al área a que pertenece.
		Las pruebas consistieron en verificar los diferentes niveles de privilegios, tanto para el sistema operativo, bases de datos, red.
		No se encontraron novedades de usuarios que se encuentren creados sin pertenecer a algún dominio o grupo de usuarios.
	Evidencias:	Lista de usuarios con privilegios asignados
		Logs se accesos de usuarios

Control	**Objetivo:**	Se debe tener en cuenta la identificación automática de terminales para autenticar conexiones a ubicaciones específicas y a equipamiento portable.
Logs del sistema operativo, reportes de módulo de seguridad de acceso de usuarios a las aplicaciones	**Alcance:**	Se deben registrar automáticamente el ingreso de los terminales al Sistema Operativo así como el final de la sesión.
	Procedimiento a cumplir:	Al Administrador de Seguridad habilita los Logs del sistema Operativo para registrar automáticamente las terminales.
	Pruebas:	Están habilitados los logs de los sistemas operativos y bases de datos, para determinar ingresos, salidas y otras actividades de los usuarios.
		Las pruebas consistieron verificar los logs del sistema operativo sobre una cuenta creada donde se realizaron ingresos y salidas del sistema.
	Evidencias:	Logs del Sistema Operativo, logs de la Base de Datos

Control	**Objetivo:**	Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable.
Se han establecido claves de identificación para cada uno de los usuarios que tienen acceso a los sistemas de información.	**Alcance:**	Verificar en una muestra significativa de usuarios para identificar tareas realizadas.
	Procedimiento a cumplir:	El Administrador de Seguridad debe asignar un identificador único al momento de su creación para el uso de cualquier recurso de información.
	Resultados:	Todos los usuarios poseen un identificador único y una contraseña asignada para el acceso a los diferentes sistemas de información.
		Las pruebas realizadas consistieron en realizar observaciones al ingreso de los usuarios al sistema desde su computador.
		El Sistema Operativo no permite identificadores de usuarios duplicados.
	Evidencias:	Logs del Sistema Operativo. Lista de usuarios.

Control	**Objetivo:**	Limitar el uso de utilitarios del sistema que podrían tener la capacidad de pasar por alto los controles del sistema.
Existen restricciones para cada equipo, para que solo se ejecuten las aplicaciones necesarias para sus labores diarias.	**Alcance:**	Verificar que solo las aplicaciones necesarias estén activas para que el usuario pueda utilizarlas.
	Procedimiento a cumplir:	El Administrador de Seguridad de acuerdo a las reglas de accesos configuradas desde el servidor, restringe el de utilitarios.
	Pruebas:	Existe creadas políticas a nivel de servidor sonde se restringe las aplicaciones que no se necesitan ejecutar o que no son necesarias.
		Se realizó pruebas ingresando en varias computadoras e intentando cambiar configuraciones de red y del sistema operativo para intentar tener acceso a otros recursos.
		No se encontraron novedades al realizar las pruebas.
	Evidencias:	Se verificó en las máquinas de los usuarios que se cumpla el control.

Control	**Objetivo:**	Las terminales inactivas en ubicaciones de alto riego, por ej. áreas públicas o externas fuera del alcance de la gestión de seguridad de la organización, o que sirven a sistemas de alto riego, deben apagarse después de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas.
Se realiza un control manual de las terminales con un tiempo de inactividad grande.	**Alcance:**	Verificar los terminales inactivos por un periodo de tiempo sean desconectadas.
	Procedimiento a cumplir:	Se debe de configurar al sistema operativo, o monitorear las terminales inactivas por un periodo largo de tiempo.
	Pruebas:	El control se lo hace manualmente al inicio de cada día, identificando que usuarios han dejado los terminales activos.
	Evidencias:	Logs de conexión de las terminales.

Control	**Objetivo:**	Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo.
Los límites están dispuesto 1 hora antes y una hora después del horario dependiendo de cada usuario.	**Alcance:**	Verificar que solo se puedan accesar a las aplicaciones dentro del horario de conexión establecido.
	Procedimiento a cumplir:	El Administrador de Seguridad debe configurar ls horarios de conexión de acuerdo a las áreas de la empresa.
	Pruebas:	A todos los usuarios se les asigna esta regla de accesos.
		Se realizó pruebas intentando ingresar al sistema después del horario normal de labores.
		No se encontraron novedades al realizar las pruebas.
	Evidencias:	Logs de transacciones efectuadas.

RECOMENDACIONES SOBRE CONTROLES INEXISTENTE

DOMINIO	OBJETIVO CONTROL	Comentarios / Observaciones	Recomendaciones
3. Política de Seguridad	Política de Seguridad de la Información	Desconocimiento de la gerencia sobre temas de seguridad informática..	La Dirección debe aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.
			Revisar regularmente la política, y en caso de cambios que tengan influencia, se debe asegurar que estos cambios deben estar aprobados.
			Realizar una declaración del propósito de los responsables del nivel gerencial, apoyando los objetivos y principios de la seguridad de la información.
		Falta de definiciones importantes en la Política provocando incidentes de seguridad significativos.	Realizar una adecuada definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo que permite la distribución de la información.

		Políticas descontinuadas y no acordes al cambio de tecnologías. Indicios de nuevas vulnerabilidades o cambios en la infraestructura técnica o de la organización	Describir una breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad, que son especialmente importantes para la organización, por ejemplo: 1) cumplimiento de requisitos legales y contractuales; 2) requisitos de instrucción en materia de seguridad; 3) prevención y detección de virus y demás software malicioso; 4) administración de la continuidad comercial; 5) consecuencias de las violaciones a la política de seguridad.
		Desconocimiento de los usuarios sobre la importancia de seguridad de la información.	Difundir la política, realizar charlas de capacitación y entrenamientos a todo el personal.
		Falta de apoyo al área de seguridad de la información	Colocar un propietario que sea el responsable de su mantenimiento y revisión para la política de seguridad de la institución.

DOMINIO	OBJETIVO CONTROL	Comentarios / Observaciones	Recomendaciones
4. ORGANIZACIÓN DE LA SEGURIDAD	Seguridad del acceso de terceras personas	Accesos físicos no autorizados de terceras personas, la razón es por la mala división de los departamentos; como ejemplo se observó que el área de desarrollo de sistemas está ubicado en la dirección de la coordinación ejecutiva y en el mismo piso se encuentra la dirección de recursos humanos y por ende existe muchas visitas externas; y el área de Telecomunicaciones se encuentra en la dirección de obras públicas.	Reestructurar el área donde se encuentra el departamento de Computo, ya que debería estar ubicado en un lugar aislado de los demás departamentos; y debe tener un guardia de seguridad de entradas y salidas al centro de computo adicional con registro de bitácoras(horas y salidas del personal).
		Accesos lógicos no autorizados de terceras personas, se observó que tienen acceso a las bases de datos pero están supervisados por una persona de la institución.	Se debe realizar un procedimiento de autorización de información sensible para uso de los terceros.
			Se recomienda crear una política de seguridad para terceras personas.

		La Institución cuenta con procesos del área IT tercializados en los cuales no se han definido en sus contratos los niveles de seguridad correctos.	En los contratos de terceras personas se debe considera las siguientes cláusulas: a) la política general de seguridad de la información. b) la protección de activos. c) una descripción de cada servicio del que podrá disponerse. d) el nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables.
			e) disposición que contemple la transferencia de personal cuando corresponda. f) las respectivas obligaciones de las partes con relación al acuerdo. g) responsabilidades con respecto a asuntos legales, por ej., legislación referida a protección de datos, especialmente teniendo en cuenta diferentes sistemas legales nacionales si el contrato contempla la cooperación con organizaciones de otros países.

		Se debe reestructurar los contratos a terceras personas y en ellos se debe contemplar una cláusula de confidencialidad de la información a la cual ellos van a tener acceso; para evitar el robo y manipulación de los mismos.	h) derechos de propiedad intelectual y asignación de derecho de propiedad intelectual, y protección de trabajos realizados en colaboración. i) acuerdos de control de accesos. j) la definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos. k) el derecho a monitorear, y revocar (impedir), la actividad del usuario. l) el derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditorías. m) el establecimiento de un proceso gradual para la resolución de problemas; también deben considerarse, si corresponde, disposiciones con relación a situaciones de contingencia.

			n) responsabilidades relativas a la instalación y el mantenimiento de hardware y software, o) una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos, p) un proceso claro y detallado de administración de cambios, q) los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos, r) los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad, s) los controles que garanticen la protección contra software malicioso, t) las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad, u) la relación entre proveedores y subcontratistas.

DOMINIO	OBJETIVO CONTROL	Comentarios / Observaciones	Recomendaciones
7. SEGURIDAD FISICA Y AMBIENTAL	Áreas de seguridad	En caso de desastres naturales especialmente los incendios; sin el mecanismo apagado automático ocasionaría más pérdidas materiales a la institución.	Tener un control de apagado automático de todos los equipos electrónicos y activación de una alarma para alertar a todo el personal.
		Accesos no autorizados a áreas de mayor cuidado.	Para el acceso a la información sensible, y a las instalaciones de procesamiento de información deben ser controlados y limitados exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por Ej. tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.
			Revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.
			En el área de computo deben estar en una ubicación discreta y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, las cuales indiquen la presencia de actividades de procesamiento de información.

		No hay una persona que controle las entradas y salidas de personas no autorizadas en las áreas de mayor cuidado como es el centro de computo ya que se encuentra ubicada en áreas de mayor presencia de visitantes externos.	Reestructurar el área donde se encuentra el departamento de Computo, ya que debería estar ubicado en un lugar aislado de los demás departamentos; y debe tener un guardia de seguridad de entradas y salidas al centro de computo adicional con registro de bitácoras(horas y salidas del personal).
		Se observó que el área de desarrollo de sistemas está ubicado en la dirección de la coordinación ejecutiva y en el mismo piso se encuentra la dirección de recursos humanos y por ende existe muchas visitas externas; y el área de Telecomunicaciones se encuentra en la dirección de obras públicas.	
		Ventanales grandes en el área de servidores, en caso de algún desastre natural, puede ocasionar accidentes o accesos no autorizados de personas. En el área de centro de computo (Servidores), tiene como medio de ingreso una puerta de madera y no tiene el dispositivo de control de tarjetas de ingreso magnético.	El área de instalaciones de procesamiento de información debe ser físicamente sólido (por Ej. no deben existir claros [o aberturas] en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por Ej., mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

		Daños e intrusiones	Implementar un adecuado sistema de detección de intrusos. Los mismos que deben ser instalados según estándares profesionales y probados periódicamente. Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. (Sala de cómputos y las salas de comunicaciones).
			Las instalaciones de procesamiento de información administradas por la organización deben estar físicamente separadas de aquellas administradas por terceros.
		Se encuentran a la vista de todo las personas que entran al departamento ya que están ubicadas al lado del teléfono como guía telefónica de Trabajo.	Implementar política personal interna por departamento, la cual indique que las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible no deben ser fácilmente accesibles al público.
		Pérdida de equipos importantes, pérdida de información y pérdida humana.	Los materiales peligrosos o combustibles que se encuentren en la institución deben ser almacenados en lugares seguros a una distancia prudencial del área protegida.

		Robo, pérdida y modificación de la información y activos.	Restringir el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información; y en caso de ser necesario se debería crear un procedimiento de acceso a las instalaciones de los mismos.
	Seguridad de los equipos	Daños de equipos por ubicación: Incendio, robos, vibraciones, polvo, humo, agua y comidas y bebidas.	Los equipos deben ser ubicados en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.
			Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.
			Los ítems que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.

			Adoptar controles para minimizar el riesgo de amenazas potenciales, por Ej. 1) robo 2) incendio 3) explosivos 4) humo; 5) agua (o falta de suministro) 6) polvo 7) vibraciones 8) efectos químicos 9) interferencia en el suministro de energía eléctrica. 10) radiación electromagnética.
		Daños de equipos o pérdida de integridad de la información por factores externos.	Considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ej. un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.
		Interferencias, daños e intrusos.	Realizar una adecuada protección en el cableado de red contra interceptación no autorizada o daño

	Controles Generales	Robo, pérdida y modificación de la información y activos.	Implementar la política de escritorio limpio, para asegurar la confidencialidad de los documentos en papel y medios informáticos.
			Implementar una política la cuál instruya a todo el personal que debe apagar las computadoras personales, terminales e impresoras o colocar una adecuada cerradura de seguridad, contraseñas u otros controles cuando no se encuentren en uso.
			Realizar un control en el uso de las fotocopiadoras, recepción y envío de correo, y las máquinas de fax y teléx.

Dominio	Objetivos de Control	Comentarios	Recomendaciones
9. Control de Accesos	Acceso de usuarios	Desconocimiento de los usuarios sobre la responsabilidad de las contraseñas en la empresa	El proceso de administración de contraseñas debe contemplar que los usuarios firmen una declaración donde se comprometan a mantener sus contraseñas personales en secreto.
			Uso de contraseñas provisionales para usuarios nuevos o quienes por algún motivo se hallan olvidado la contraseña. Esta debe modificarse inmediatamente una vez identificado el usuario
			La asignación de contraseñas provisionales deben otorgarse a través de algún medio seguro, exceptuando terceras personas.
			Las contraseñas deben almacenarse en forma cifrada y en medios donde el acceso solo esté a cargo de personal autorizado.
		Asignación de accesos a usuarios sin firmas de responsabilidad o autorización	Revisión de los derechos de acceso de los usuarios a intervalos regulares cada 6 meses y después de cada cambio
			Revisión de las autorizaciones de privilegios especiales de derechos de acceso cada 3 meses

			Revisión de las asignaciones de privilegios a intervalos regulares cada 6 meses
	Responsabilidades del usuario	Divulgación de contraseñas, fáciles de identificar, contraseñas iguales para varios usuarios	Se debe comunicar a los usuarios que deben cumplir los puntos de seguridad de la contraseña.
	Responsabilidades del usuario		Mantener las contraseñas en secreto.
			Evitar mantener un registro en papel de las contraseñas, a menos que este pueda ser almacenado en forma segura;
			Cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas;
			Seleccionar contraseñas de calidad, con una longitud mínima de seis caracteres que:
			1) sean fácil de recordar;
			2) no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por Ej. nombres, números de telé-fono, fecha de nacimiento, etc. ;
			3) no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o total-mente alfabéticos.

			Cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuentas con privilegios deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas
			Cambiar las contraseñas provisionales en el primer inicio de sesión
			No incluir contraseñas en los procesos automatizados de inicio de sesión, por Ej. aquellas almacenadas en una tecla de función o macro.
			No compartir las contraseñas individuales de usuario
	Responsabilidades del usuario	Accesos no autorizados a equipos e información	Se debe notificar a los usuarios que deben cumplir con los siguientes puntos:
			Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por Ej. un protector de pantallas protegido por contraseña ;
			Llevar a cabo el procedimiento de salida de los procesadores centrales cuando finaliza la sesión (no solo apagar la PC o terminal) ;

			Proteger las PCs o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ej. contraseña de acceso, cuando no se utilizan.
		Accesos no autorizados debido a la facilidad del sistema o de los mensajes mostrados.	No desplegar identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión;
			Desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder a la computadora ;
			No dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión ;
			Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta ;
			limitar el número de intentos de conexión no exitosos permitidos (se recomiendan tres) y considerar:

	Responsabilidades del usuario		Registrar los intentos no exitosos.
			Implementar una demora obligatoria antes de permitir otros intentos de identificación, o rechazar otros intentos sin autorización especifica ;
			Desconectar conexiones de data link
			Limitar el tiempo máximo y mínimo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión ;
			Desplegar la siguiente información al completarse una conexión exitosa:
			Fechas y hora de la conexión exitosa anterior;
			Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.
	Control de acceso al sistema operativo	Contraseñas poco confiables y fácilmente descifrables	Un buen sistema de administración de contraseñas debe:
			Imponer el uso de contraseñas individuales para determinar responsabilidades;

			Cuando corresponda, permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso;
			Imponer una selección de contraseñas de calidad.
			Cuando los usuarios mantienen sus propias contraseñas, imponer cambios en las mismas.
			Cuando los usuarios seleccionan contraseñas, obligarlos a cambiar las contraseñas temporarias en su primer procedimiento de identificación
			Mantener un registro de las contraseñas previas del usuario y evitar la reutilización de las mismas ;
	Control de acceso al sistema operativo		No mostrar las contraseñas en pantalla, cuando son ingresadas
			Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación;
			Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional ;

			Modificar las contraseñas predeterminadas por el vendedor, una vez instalado el software
		Accesos no autorizados bajo presiones de personal mal intencionado.	Debe considerarse la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción en las áreas de atención al público

PARTE IV

DECLARACION DE APLICABILIDAD

Una vez realizado la Evaluación y Gestión de Riesgos y de acuerdo a los resultados obtenidos es necesario realizar la Declaración de Aplicabilidad con el fin de seleccionar los controles de seguridad a implementar justificando el porqué son apropiados para la organización. Así mismo se indica que controles no se escogen o no son importantes indicando su respectiva justificación.

Para el presente proyecto entregamos la Declaración de Aplicabilidad como una recomendación, para que la organización evalúe, la apruebe y autorice su posterior implementación. En la tabla a continuación se han considerado sólo los dominios y objetivos de control más críticos de acuerdo a la Evaluación de Riesgos realizada.

Sección	Objetivo		Control	Aplicación Si / No	Referencia o Justificación de la exclusión
3	**POLÍTICA DE SEGURIDAD**				
A.3.1	Política de Seguridad de Información	A.3.1.1	Documentar políticas de seguridad de información	Si	La política de seguridad debe estar documentada y difundida al personal de la empresa, para garantizar su cumplimiento.
		A.3.1.2	Revisión y evaluación	Si	Le revisión y evaluación de la política debe realizarse con el fin de mantenerla actualizada de acuerdo al cambios organizacionales o de tecnología.
4	**ORGANIZACIÓN DE LA SEGURIDAD**				
A.4.2	Seguridad del acceso de terceras personas	A.4.2.1	Identificación de riesgos de acceso de terceras personas	Si	Control necesario debido a que existen contratos con terceros, tanto personal técnico como desarrollo.

		A.4.2.2	Requerimientos de seguridad en contratos con terceras personas	Si	Dentro de los contratos con los terceros se deben establecer cláusulas para salvaguardar los activos a los que tengan acceso.
A.4.3	Abastecimiento Externo (Tercerización)	A.4.3.1	Requerimientos de seguridad en los contratos	No	El procesamiento de la información es realizado por personal de la empresa y dentro de la misma.

7	**SEGURIDAD FÍSICA Y DEL AMBIENTE**				
A.7.1	Áreas de seguridad	A.7.1.1	Perímetro de seguridad física	Si	El centro de procesamiento de información debe estar protegido en su perímetro completamente para evitar daños o pérdidas materiales.
		A.7.1.2	Controles de entrada físicos	Si	El control existe y está implementado correctamente.
		A.7.1.3	Oficinas habitaciones y medios de seguridad	Si	El control existe y está implementado correctamente.
		A.7.1.4	Desarrollo de tareas en áreas protegidas	Si	Control necesario para evitar accesos de personal local y tercerizado no autorizados a áreas restringidas.

		A.7.1.5	Aislamiento de las áreas de entrega y carga	Si	Control necesario para evitar que personal no autorizado ingrese a las áreas de procesamiento de información.
A.7.2	Seguridad del Equipo	A.7.2.1	Ubicación y protección del equipamiento	Si	Control para mitigar riesgos de daños de equipos por ubicación: Incendio, robos, vibraciones, polvo, humo, agua y comidas y bebidas.
		A.7.2.2	Suministro de energía	Si	Controles de suministros de energía y mecanismos alternos para evitar los cortos imprevistos.
		A.7.2.3	Seguridad en el cableado	Si	Control para minimizar riesgos de Interferencias, daños e intrusos.
		A.7.2.4	Mantenimiento de equipo	Si	Controles de mantenimiento de equipo e historial de reparaciones de equipos por departamento.
		A.7.2.5	Seguridad del equipamiento fuera del ámbito de la organización	Si	Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.
		A.7.2.6	Baja segura o reutilización de equipamiento	Si	Control importante para minimizar riesgo de pérdida de confidencialidad de la información.

A.7.3	Controles Generales	A.7.3.1	Política de pantalla y escritorio limpio	Si	Este control es necesario con el fin de que los usuarios eviten dejar información sensible tanto en los escritorios como en las computadoras al dejar la oficina o lugar de trabajo.
		A.7.3.2	Retiro de bienes	Si	Control de entradas y salidas de los equipos las cuales tienen firmas de responsables, en este caso la coordinación, el director de área y el responsable del control del edificio.

9	**CONTROL DE ACCESOS**				
A.9.2	Administración del acceso del usuario	A.9.2.1	Registros del usuario	Si	Actualmente el control existe pero debe mejorar su implementación para cumplir su objetivo
		A.9.2.2	Administración de privilegios	Si	El control existe y está funcionando correctamente
		A.9.2.3	Administración de contraseñas de usuario	Si	Este control debe de implementarse formalmente, para asegurar que el usuario mantenga su propia contraseña, garantizar que se mantenga en secreto.

		A.9.2.4	Revisión de los derechos de acceso del usuario	Si	La implementación de este control ayudará a minimizar riegos de accesos no autorizados por errores en creación de privilegios o modificaciones sin autorización.
A.9.3	Responsabilidad del usuario	A.9.3.1	Uso de contraseña	Si	Este control es importante para minimizar los riesgos de contraseñas fáciles de identificar o duplicadas, concientizando al usuario sobre su responsabilidad.
		A.9.3.2	Equipos desatendidos en áreas de usuarios	Si	Este control es necesario para evitar accesos no autorizados cuando los usuarios dejen sus equipos por un largo tiempo para evitar accesos no autorizados.
A.9.5	Control de Acceso al Sistema de Operación	A.9.5.1	Identificación automática de terminales.	Si	Actualmente el control existe y está funcionando correctamente.
		A.9.5.2	Procedimientos de conexión de terminales	Si	Para evitar accesos no autorizados debido a la facilidad del sistema o de los mensajes mostrados.
		A.9.5.3	Identificación y autentificación del usuario.	Si	El control existe y está funcionando correctamente
		A.9.5.4	Sistema de administración de contraseñas	Si	Este control es necesario para evitar contraseñas poco confiables y fácilmente descifrables

		A.9.5.5	Uso de Utilidades del sistema.	Si	El control existe y está funcionando correctamente
		A.9.5.6	Alarmas silenciosas para la protección de los usuarios	Si	Este control es necesario para aquellos usuario que manejan información sensible y con contacto con el público
		A.9.5.7	Desconexión de terminales por tiempo muerto	Si	El control existe pero la implementación no es eficiente debido a que el control es manual y no hay un procedimiento formal para realizarlo.
		A.9.5.8	Limitación del horario de conexión	Si	Este control existe y está implementado correctamente.

PARTE V

Recomendaciones Generales

- Todo Sistema de Gestión de Seguridad de la Información requiere principalmente el apoyo de alta dirección con el fin de que exista el compromiso a nivel de toda la organización. En el caso del Consejo Provincial del Guayas esto debe provenir desde el Prefecto hasta todas las Direcciones Administrativas
- La seguridad de la información es una responsabilidad de la empresa compartida por todos los miembros del equipo gerencial. Por consiguiente, debe tenerse en cuenta la creación de un foro gerencial para garantizar que existe una clara dirección y un apoyo manifiesto de la gerencia a las iniciativas de seguridad.
- Se recomienda que el área de Informática goce de total independencia, a nivel de Dirección; para garantizar su objetividad y función dentro de la Institución.
- Para un adecuado mantenimiento del SGSI, el Consejo Provincial debe considerar los siguientes roles dentro se su organización:
    - **Oficial de Seguridad**: persona que está a cargo de la implementación del SGSI y su respectivo mantenimiento y deberá coordinar junto con los jefes de cada área los controles a implementar.
    - **Administrador de Claves**: persona cuya actividad principal derá de asegurar que cada una de los usuarios de los sistemas de información posee autorización para el uso de los recursos asignados.
    - **Auditor de Sistemas**: persona con perfil de auditor de sistemas para verificar que los controles se mantengan y salvaguardar los activos de información de la organización.
- Se debe asignar e identificar a los propietarios para todos los activos importantes dentro del Consejo Provincial del Guayas y se debe asignarse la responsabilidad por el mantenimiento de los controles a implementar.
- Como se ha indicado anteriormente la implementación de un SGSI dentro de una organización requiere que se involucre todas las unidades administrativas. En la siguiente tabla indicamos una recomendación sobre en que contextos se requiere la participación de las diferentes áreas.

Domino	Área involucrada (Principales)
Política de Seguridad	Prefectura Dirección Financiera Dirección Administrativa Dirección de RRHH Coordinación de Sistemas
Organización de la Seguridad	Prefectura Dirección Financiera Dirección Administrativa Dirección de RRHH Coordinación de Sistemas
Clasificación y Control de Activos	Dirección Financiera Coordinación de Sistemas Auditoría Interna Departamento Legal
Seguridad del Personal	Dirección Financiera Dirección de Recursos Humanos Coordinación de Sistemas Auditoría Interna Departamento Legal
Seguridad Física y Ambiental	Dirección Financiera Dirección de Recursos Humanos Coordinación de Sistemas Coordinación de Seguridad
Administración de Operaciones y Comunicaciones.	Dirección Financiera Dirección de Recursos Humanos Coordinación de Sistemas Coordinación de Seguridad
Control de Accesos	Dirección Financiera Coordinación de Sistemas Auditoría Interna
Desarrollo y Mantenimiento de Sistemas	Coordinación de Sistemas Auditoría Interna

Administración de la Continuidad del Negocio	Todas las Áreas del Consejo Provincial del Guayas
Cumplimiento	Dirección de RRHH Coordinación de Sistemas Departamento Legal Auditoría Interna

- Se deben llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles una vez implementados a fin de:

    a. reflejar los cambios en los requerimientos y prioridades de la empresa;
    b. considerar nuevas amenazas y vulnerabilidades;
    c. corroborar que los controles siguen siendo eficaces

PLAN DE ACCIÓN

PLAN DE ACCIÓN

Dominio	Objetivos de Control	Tiempo	Responsables
Política de Seguridad	Política de Seguridad de Infromación	2 meses	Principal: Coordinador de Informática, Jefe de Seguridad Secundarios: todos los miembros de la organización.
Organización de la Seguridad	Seguridad de Acceso de Terceras Personas	2 meses	Coordinador de Informática, Jefe de Securidad, Sindico Provincial, Jefe de Mantenimiento del edificio
Control físico y ambiental	Areas de Seguridad Seguridad de los Equipos Controles Generales	6 meses	Jefe de seguridad, jefe de mantenimiento del edificio, coordinador de informática, director financiero
Control de accesos	Administración de Accesos de Usuarios Responsabilidades del Usuario Control de Acceso al Sistema Operativo	4 meses	Jefe de Redes, Jefe de Seguridades

Conclusión

La Seguridad es un proceso que afecta a toda la organización y está basado principalmente en las personas que la conforman.

Las organizaciones deben definir una estrategia de seguridad basada en el negocio y no en la tecnología.

La seguridad que proporciona un SGSI es permanente puesto que es un proceso, y no acciones puntuales.

El enfoque de la Seguridad debe ser integral, si no puede conducir a una falsa sensación de seguridad y al fracaso

Esperamos que el presente proyecto coadyuve de forma significativa al H. Consejo Provincial del Guayas a obtener los objetivos de seguridad esperados para el año en curso, estamos seguros que servirá de base y guía para el tratamiento y gestión de riesgos la Institución, así como para mejorar los parámetros de confidencialidad, integridad y disponibilidad de la información.

El diseño del presente Sistema de Gestión de Seguridad de la Información, marcará ventajas tecnológicas y competitivas, siendo el soporte de la definición de políticas, normas, procesos y procedimientos que serán ejecutados en la siguiente etapa de implementación y sobre todo podrá ser utilizado por la Institución como base para una certificación en seguridad de la información con la norma BS 7799-2.

Gracias.

Bibliografía

Normas técnicas sobre Sistemas de Gestión de la Seguridad de la Información (SGSI) INCONTEC

Norma Técnica Colombiana NTC – BS- 7799- 2

Norma Técnica Colombiana NTC – ISO / IEC 17799

Código de Buenas Prácticas para la Gestión de la Seguridad de la Información

Manual de preparación para la certificación CISA- ISACA (www.isaca.org, ww.isaca.org.ec)

Auditoria Interna Moderna de Brink &¨Witt

Sistemas de Información para la Gestión Empresarial: Procedimientos, Seguridad y Auditoría de Alberto R. Lardent, Pentice Hall

ANEXOS

ANÁLISIS DE LA SITUACIÓN TECNOLÓGICA ACTUAL DE LA INSTITUCIÓN

DOMINIO	NORMA	PROGRAMA DE AUDITORÍA	Si	No	COMENTARIO	JUSTIFICACIÓN
Política de Seguridad	Política de Seguridad de la Información	Existe una política de seguridad en la Institución?	x		Existencia de políticas de acceso a la red de datos y políticas de acceso a Internet.	En este dominio la Institución se encuentra en el nivel 1 ya que si bien es cierto existe una política de seguridad, esta no abarca todos los parámetros de seguridad mínimos que deben ser considerados en la construcción de una política de seguridad, así como no es aprobada por la alta gerencia y no se actualiza de forma continua. Entre los parámetros de seguridad con los que cuenta la política actual podemos mencionar: Políticas de acceso, políticas de contraseña, responsabilidades de Directores y Jefes departamentales, políticas en el uso de los servicios.
		Dicha política es aprobado por la alta gerencia?		x	Es aprobada por el Coordinador de Informática.	
		La política de seguridad existente es completa?		x	Cumple con ciertos aspectos de seguridad.	
		La política de seguridad es conocida por todos los miembros de la Institución?		x		
		Existen procedimientos de revisión y evaluación?		x	La política no se actualiza adecuadamente.	
Organización de la seguridad	Infraestructura de seguridad de información	Existe un comité de dirección sobre seguridad de información?		x	La seguridad es evaluada internamente por cada jefe de área de la Coordinación de Informática.	La Institución en este dominio se encuentra en el nivel 0, no existe comité de dirección de seguridad de la información, el responsable de seguridad se encuentra ejecutando otras funciones no inherentes a su cargo. La Institución cuenta con procesos del área IT tercializados en los cuales no se han definido en sus contratos los niveles de seguridad correctos.
		Existe un oficial de seguridad de información?	x		No existe una adecuada segregación de funciones, el responsable de seguridades está a cargo de otra área.	
		Se cuenta con asesoria de un especialista en seguridad de la información?		x		
	Seguridad de acceso de terceras personas	Existen procesos del área IT tercializados?	x		Se encuentran tercializados el área de desarrollo y de mantenimiento de hardware.	
		Existen definición de niveles de seguridad definidos formalmente en contratos con terceros?		x		
	Abastecimiento Externo	No aplica				
Clasificación y control de activos	Responsabilidad por los activos	Existe un inventario de activos?	x		El inventario es revisado y actualizado cada año.	La Institución se encuentra en un nivel 1, existe un inventario de activo, pero no existen procedimientos formales para la clasificación de la información.
	Clasificación de la información	Existe la clasificación de la información?		x	No existe procedimiento formal para la clasificación de la información, pero se identifica la información confidencial.	
Seguridad del personal	Seguridad en la definición del trabajo y el abastecimiento	Existen políticas de personal claramente definidas?		x	No se establecer procedimientos de verificación de datos al momento de la contratación del personal, tanto para personal permanente como para personal temporal.	La Institución se encuentra en este dominio en un nivel 1, la falta de procedimientos formales de capacitación e inducción de la seguridad, así como no contar con políticas de personal adecuada y funciones claramente definidas y actualizadas puede conllevar a serios problemas de seguridad. Si bien es cierto existen responsabilidades definidas para el manejo de incidentes y se emiten reportes para informar del mal funcionamiento del software; estos procedimientos no son formales ni se encuentran documentados; lo que califica a la Institución en un nivel 1 de estado actual con respecto a la seguridad del personal.
		Existen políticas de confidencialidad definidas en los contratos de personal interno?		x		
		Existe un procedimiento de selección de personal?		x		
		Existe un manual de funciones claramente definido?	x		No incluye responsabilidad para mantener la política de seguridad y se encuentra desactualizado	
	Capacitación del usuario	Los usuarios son correctamente inducidos sobre temas de seguridad?		x	Existe entrenamiento sobre los recursos de procesamiento de información pero no existe una completa capacitación sobre los requisitos de seguridad, políticas y procedimientos organizacionales.	
		Existe capacitación sobre los recursos de procesamiento de la información?	x			
	Responder a los incidentes y malfuncionamientos en la seguridad	Existen reportes de incidentes de seguridad?		x	No existe una política que haga referencia a la emisión de reportes de incidentes de forma obligatoria, existen procedimientos informales en la emisión de comunicados en referencia a incidentes de seguridad.	

		Existen repotes de debilidades de seguridad?		x		

Seguridad del personal		Existen reportes de las anomalías del software?	x		Las anomalías del software son comunicadas por los usuarios y dueños de las aplicaciones a la Coordinación de Informática mediante oficios formales.	
		Existe procesos disciplinarios para lo empleados que violen las políticas y procedimientos de seguridad de la información?		x		
Seguridad física y ambiental	Áreas de seguridad	Se utilizan perímetros de seguridad para protección de las instalaciones de procesamiento de la información?		x		La Institución se encuentra en un nivel 1, ya que existen esquemas de seguridad sobre el centro de procesamiento y equipos, pero los controles son insuficientes. Así mismo no existen procedimientos formales de seguridad para el resguardo de la información, las políticas al respecto son inexistentes.
		Existen medios de control de acceso físico al edificio y al lugar de procesamiento de la información?	x		Existen controles magnéticos de accesos físicos al edificio y en la puerta principal del piso, más no para el acceso al centro de cómputo.	
		Existen entradas no autorizadas o contaminación del entorno del lugar de procesamiento de la información?		x		
		Existen registros de visitas (entradas y salidas) al lugar del procesamiento de la información?		x	No existen bitácoras de ingresos y salidas del centro de cómputo, ni de las áreas de procesamiento de la información.	
		Se mantienen controladas las áreas de despacho y de cargas de energía?	x			
	Seguridad del equipo	Los equipos se encuentran en lugares seguros?		x	No en su totalidad, existen áreas en las cuales los equipos pueden ser accedidos fácilmente.	
		Los equipos están protegidos contra fallas de suministros y anomalías eléctricas?		x	No todos los equipos cuentan con UPS y no existe un UPS general para mantener y soportar la descarga eléctrica.	
		El cableado eléctrico y de datos se encuentra protegido?	x			
		Existe mantenimiento preventivo y correctivo a los equipos?	x			
	Controles Generales	Existen políticas de escritorio limpio?		x	Se observó en las instalaciones la falta de archiveros y segruidad en cuanto al resguardo de la documentación.	
		Existen controles de bloqueo de pantalla?		x	Existen bloqueos manuales al acceso al sistema operativo y controles automáticos que inhabilitan las aplicaciones por periodo de inactividad.	
Gestión de comunicaciones y operaciones	Procedimientos y responsabilidades operacionales	Existen procedimientos de operación identificados y documentados?		x		Los controles y procedimientos de la gestión de redes y operaciones en la Institución son insuficientes ya que existen procedimientos no documentados, incompatibilidad de funciones comos las ya mencionadas y las prácticas realizadas con respecto a los respaldo de la información no grantizan la seguridad de las misma. Existen controles referentes a detección y eliminación de software malicioso y se realizan monitoreos sobre la demanda de capacidad instalada, todo lo referente puede indicar que la Institución se encuentra en un nivel 1 en lo que respecta a la gestión y operación de redes.
		Se controlan los cambios en las instalaciones y sistemas de procesamiento de la información?	x		Existen procedimientos no formales cuando se realizan cambios en las instalaciones y sistemas de procesamiento de la información; responden comúmente a programas de trabajos elaborados a medida de la ocurrencia de un cambio.	
		Existen controles de cambios en los programas?	x			
		Existen registros de auditorias de cambios en los programas?	x		Los cambios o modificaciones a los programas se guardan en registros de auditorías.	
		Existen responsabilidades y procedimientos para la administración de incidentes?	x		Pero dichas responsabilidades y procedimientos no han sido documentados ni formalizados.	

		Existe la correcta segregación de funciones entre los miembros de la institución?		x	Existen funciones incompatibles, el administrador de redes ejecuta funciones de administrador de base de datos y otras funciones inherentes al área de seguridad. Las funciones de operador la ejecutan varios miembros de los departamentos de redes, técnico y desarrollo.	

		Existe separación del ambiente de desarrollo y producción?	x		Los ambientes de producción y desarrollo se encuentan debidamente separados y administrados en servidores diferentes.	
	Planeación y aceptación del sistema.	Se realizan seguimientos a las demandas de capacidad?	x		Existe monitoreo constante del estado de la capacidad.	
		Se establecen procedimientos para aceptación de sistemas informáticos nuevos?	x		El procedimiento se encuentra documentado y aprobado.	
		Se realizan las pruebas correspondientes para la aceptación de los nuevos sistemas?	x		Las pruebas son ejecutadas en la etapa de implementación, pero no existe documentación de los parámetros a tomar en cuenta en las pruebas de los sistemas.	
Gestión de comunicaciones	Protección contra software malicioso	Existen controles de detección y prevención para protección de software malicioso?	x		Existe software antivirus coorporativo, el cual se instala en todos los computadores pertenecientes a la red de la nstitución. No existe estandarización para aquellos equipos que no pertenecen a la red, incluso existen equipos bajo ésta característica que no poseen antivirus instalados.	
	Gestión en casa.	Existen políticas de respaldo definidas y cumplidas?	x		Existen políticas de respaldo diarias de los datos.	
		Las copias de respaldo mantienen una adecuada protección física?		x	Las copias de respaldo de los datos son almacenadas en el servidor; no existe procedimientos formal de respaldo en medios magnéticos.	
		Se realizan pruebas para asegurar el funcionamiento de las copias de respaldo?		x		
		Existen bitácoras de operador en el manejo de respaldos?	x		Por medio de un control manual se realiza un control sobre el manejo de los respaldos, incidentesy novedades diarias.	
	Administración de redes	Existen procedimientos para la gestión de equipos remotos?	x		Existencia de procedimientos no formales para el uso de equips remotos.	
		Existen documentación de los sistemas de información?	x			
		Existen políticas del uso de Internet y correo electrónico?	x		Existen consideraciones en la política de seguridad definida por la Institución que hacen referencia al uso de Internet y Correo Electrónico.	
Control de Accesos	Control de acceso	Está definida una política de accesos para la organización donde están definidos las reglas y derechos del control de accesos de los usuarios de la organización	x		Se encuntran definidas en la política de seguridad.	En este dominio la Institución se encuentra en el nivel 1, existen procedimientos con respecto a los controles de acceso, pero muchos de esos procesos no han sido formalizados y son desconocidos por los usuarios finales. Existen claros indicios de establecimiento de controles de accesos en la Institución, sobre todo los accesos para los servicios de red y las aplicaciones; pero debido a la importancia de minimizar los riesgos con respecto a la pérdida de confidencialidad y disponibilidad de la información deberían establecerse los controles necesarios y adecuados para garantizar de forma más eficiente los accesos.
		Existen reglas de acceso diferenciadas entre obligatorias y condicionales?		x		
	Administración de accesos de usuarios	Existe un procedimiento formal de registros de altas y bajas de usuarios a los sistemas de información.	x		Existe un procedimiento formal y estipulado dentro de la organización pero que no es conocido por todos los miembros.	
		Se administra los privilegios de acceso a los usuarios para impedir accesos no autorizados.	x			

		Existe un procedimiento formal para la administración de asignación de contraseñas a usuarios		x		
		Existe un proceso formal de revisión de los controles de accesos a datos y servicios de TI y a intervalos regulares.		x	En cierto casos el Director de Área solicita la revisión de accesos de los usuarios de área, pero esto no es un procedimiento formalmente establecido.	
	Responsabilidades del usuario	Los usuarios siguen buenas prácticas de seguridad en la selección y uso de contrasenas.		x		

Control de Accesos		Se garantiza la seguridad de los equipos desatendidos durante un periodo extenso por los usuarios, mediante notificaciones sobre puntos a cumplir	x		Existen controles manuales y automáticos para bloqueo de equipos desatendidos.	
	Control de acceso a la red	Existe una política sobre el uso de redes y servicios de red, para garantizar que los usuarios cuentan con acceso sólo para lo que han sido autorizados.	x			
		Existen ruteos fozosos para que los usuarios no tengan acceso servicios de red que no tengan autorización y limitar el acceso sólo a recursos necesarios.		x		
		Existen procesos de autenticación para usuarios de conexiones remotas		x		
		Los nodos de conexión remota son autenticados, para garantizar el acceso a grupos de usuarios.		x		
		Existen puertos de diagnóstico remotos protegidos contra accesos no autorizados.	x			
		Existen subdivisiones de redes para separar lógicamente grupos de usuarios y controlar accesos no autorizados a los recursos.	x			
		Existen controles de conexión a la red para limitar la capacidad de conexión de los usuarios.		x		
		Existen controles de ruteos de redes para evitar accesos no autorizados a usuarios externos de redes compartidas.	x			
		Existen controles para garantízar las seguridades en el servicio de red del proveedor.		x		
	Control de acceso al sistema operativo	Existen controles para identificar automáticamente los terminales que inician sesión en el sistema.	x			
		Existen procedimientos de control de conexión de terminales para minimizar la oportunidad de acceso no autorizado.	x			
		Todos los usuarios poseen un identificador único y exclusivo de acceso y autenticación, de modo que se puedan establecer responsabilidades de las actividades realizadas y que puedan ser rastreadas.	x			
		Existen algún sistema de administración de contraseñas que garantize contraseñas de calidad	x			
		Está controlado el uso de utilitarios de sistemas para evitar que pasen por alto los controles se sistemas y aplicaciones.	x			

		Existen alarmas silenciosas como medio de protección a usuarios.		x		
		Las terminales inactivas en ubicaciones de riesgo se apagan después de un periodo de inactividad para evitar acceso de personas no autorizados.		x		
		Existe un límite de horario de conexión para nrindar seguridad adicional en aplicaciones sensibles o de alto riesgo.	x			
	Control de acceso a las aplicaciones	Existe restricciones de acceso a la información a los usuarios de acuerdo a las necesidades de la organización y conforme a las políticas definidas.		x		
		Existe aislamiento de aquellos sistemas que son sensibles a pérdidas potenciales, controlando que sólo se compartan recursos con aplicaciones confiables.	x			
	Monitoreo del acceso y uso de los sistemas	Existen registros de auditoría de eventos donde consten excepciones y otras actividades de seguridad durante un tiempo definido para futuras investigaciones.	x			
		Existen procedimientos para monitorear el uso de instalaciones de procesamiento de infromación para garantizar que los usuarios solo están desempeñando actividades autorizadas.		x		
		Se realizan periódicamente revisiones de los resultados de las actividades de monitoreo.		x		
		Se realizan revisones de los registros de eventos significativos de seguridad por personal independiente de las áreas en monitoreo.		x		
		Existen procedimientos para sincronizar los relojes de las computadoras para garantizar exactitud de los registros de auditoría.		x		
	Computación móvil y trabajo remoto	Existen controles para que la información contenida en dispositivos móviles no puedean ser fácilemnte accesada en caso de robo o pérdida del mismo.	x			
		Existen procedimientos para proteger y actualizar los dispositivos móviles de software malicioso	x			
		Existen procedimientos de protección físicas de los equipos para evitar robo o pérdidas del mismo.		x		
		Existe protección del sitio remoto de acceso contra robo del equipo e información, divulgación no autorizada de información, acceso remoto no autorizado y el uso inadecuado de los dispositivos e instalaciones.		x		
Desarrollo y mantenimiento de sistemas	Requerimientos de seguridad de los sistemas	Se encuentran definidos los requisitos de seguridad para el desarrollo de las aplicaciones?	x		El proceso de desarrollo se encuentra tercializado, por lo cual se han definido parámetros de seguridad mínimos y parámetros de operación de las aplicaciones.	
		Estos requisitos de seguridad son claramente definidos antes de desarrollar los sistemas?	x			
	Seguridad en los sistemas de aplicación	Se validan los datos de entrada en los sistemas de aplicación?	x			

Desarrollo y Mantenimiento de Sistemas		Se realizan revisiónes periodicas de los datos para comprobar su validez e integridad?	x		Dichas evaluaciones son realizadas por los responsables departamentales; existen procedimientos de revisiones periodicas de los datos.	Existe conciencia a en parte de la organización de la seguridad con respecto al uso y manejo de los sistemas de información, se reconoce la propiedad sobre los datos en un grupo de personal de cada departamento o Dirección, los cuales son encargados de la ejecución de revisiones periodicas sobre la validez e integridad de los mismos.Existen procedimientos establecidos de control de cambios y los requerimientos para la ejecución de los mismos se realizan formalmente, pero no a nivel de toda la organización; no existe seguridad en la administración de los datos de prueba y procedimientos establecidos para su utilización y eliminación; lo que ubica a la organización en un nivel 2 en este dominio.
		Se establecen controles correspondientes para la verificación o el cuadre de archivos de las aplicaciones?	x			
		Se realizan validaciones de los datos generados por el sistema?	x			
	Controles de Criptografía	No aplica				
	Seguridad de los archivos del sistema	Existe un responsable cuando se produce un cambio en el sistema operativo por implementación de sistemas?	x		El responsable es claramente identificado a nivel de toda la organización.	
		Los sistemas operativos tienen únicamente código ejecutable de los sistemas de información?	x		Los usuarios tienen acceso únicamente a los archivos ejecutables de las aplicaciones.	
		Los datos que son utilizados de pruebas son debidamente controlados y protegidos?	x			
		Los programas de desarrollo o mantenimiento se ubican en las librerias operativas de programa fuente?		x	El ambiente de desarrollo o mantenimiento se encuentra aislado de las librerias operativas de programas fuentes de producción.	
		La información que es usada para pruebas se borra completamente después de su uso?		x	No existe procedimiento formal para eliminar las pruebas despues de su uso, en ciertos casos los datos pruebas son borrados y en otros no.	
		Se mantienen registros de auditoría de las copias de información y su uso?		x		
	Seguridad en los procesos de desarrollo y apoyo	Existen procedimientos formales de control de cambios?	x		El proceso de cambio se encuentra documentado y aprobado.	
		Los cambios los realiza el personal autorizado?	x			
		Existe aprobación o requerimiento formal antes de la ejecución de un cambio?	x		Los requerimientos formales provienen de oficios o memos enviados de las Direcciones, o son procedentes de actas de reuniones; otros requerimientos son realizados por el personal del área de Coordinación de Informática, los cuales se documentan en un sistema de órdenes de proceso.	
		Si realiza un análisis de impacto antes de la ejecución de cambios?		x		
		Existen acuerdos bajo licencias, propiedad de código y derechos de propiedad intelectual del software desarrollado por terceros?	x		Los acuerdos se encuentran en las propuestas de los contratos por tercero las cuales se adjuntan a los contratos, pero los contratos no presentan clausulas exclusivas referentes a lo mencionado.	

		Existen registros contractuales sobre la calidad del software?		x		
Administración de la continuidad del negocio	Aspectos de la gestión de la Continuidad del negocio.	Existe un proceso formal de gestión de la continuidad del negocio?		x	Los procedimientos son parciales e informales y corresponden a ciertas áreas de la gestión de la Coordinación de Informática como por ejemplo los procedimientos de contingencias sobre servidores de producción y desarrollo, así como la administración del hardware de almacenamiento.	La evaluación establecida sobre este punto nos demuestra que la Institución tiene una visión parcial de planes de contingencia y continuidad del negocio, los cuales son casi nulos así como los procedimientos formales sobre el mismo. La administración tiene conciencia sobre los riesgos pero no han existido hasta el momento evaluación de vulnerabilidades, análisis de amenazas e impacto. La respuesta ante incidentes han sido reactivas e improvisada; lo que demuestra que la Institución se encuentra en un nivel 1.
		Se ha realizado un análisis de consecuencias ante desastres naturales, accidentes, fallos de equipos?		x	Se ha realizado de forma parcial y aislada.	
		Existen procedimientos para evaluación de riesgos?		x		
		Existen planes documentados de continuidad del negocio?		x		
		Los planes de continuidad son regularmente actualizados?		x		
		Existe un comité de seguridad de la información que sea responsable de coordinar l proceso de continuidad del negocio? O un responsable claramente identificado de dicha tarea?		x		
		Los planes de continuidad son debidamente probados?		x		
Cumplimiento	Cumplimiento con requerimientos legales	Se encuentran claramente establecidos los derechos de propiedad intelectual y derecho de copia del software o de los sistemas de información?		x	No existe una definición formal en los contratos, pero sí en los acuerdos especificados en las propuestas por terceros que son anexadas a los contratos.	El cumplimiento con las leyes y reglamentaciones se cumple parcialmente, no se definen en los contratos clausulas de confidencialidad, adicionalmente la Institución puede estar haciendo uso de software sin licencias. Incluso existiendo verificaciones para el cumplimiento de leyes y reglamentaciones y manteniendo resgistros de auditorias sobre los accesos, la Institución se encuentra en un nivel 1.
		Existen normas establecidas sobre la adquisición de productos de software?		x		
		Se establecen controles para asegurar que no se sobrepase el límite de usuarios permitidos para la utilización de software?	x		Los controles son insuficientes y en determinados casos no se cumplen, como en el caso de utilización de sistemas operativos y herramientas como utilitarios.	
		Se instala únicamente software autorizado y productos bajo licencia?		x		
		Existen clausulas de confidencialidad estipuladas en los contratos?		x		
	Revisiones de política de seguridad y cumplimiento técnico	Se realizan revisiones regulares a los propietarios de los sistemas de información sobre la conformidad con las políticas, normas y cualquier otro procedimiento de seguridad?	x		Dichas revisiones son realizadas por la función de auditoría interna en la Institución.	
		Se verifica el cumplimiento de los sistemas de información con las normas de implementación de seguridad?	x		Se solicitan pruebas de acceso y seguridad de los sistemas de acuerdo a los requerimientos de la Institución y parámetros de seguridad establecidos.	
		Estas verificaciones son realizadas por personal con las competencias técnicas necesarias para asegurar el cumplimiento?	x			
	Consideraciones de auditoria de Sistemas	Los requisitos de auditoría se aprueban con la Dirección apropiada?		x		

Cumplimiento		Los accesos son registrados y supervisados?	x		Los accesos sobre aplicaciones, sistemas operativos y otros son registrados, monitoreados y supervisados por el personal correspondiente; en el caso de aplicaciones de carácter crítico se ha permitido que el nivel de supervisión sea compartido por el dueño de la aplicación.	
		Los registros de auditoria se encuentran debidamente asegurados para evitar accesos no autorizados?		x	Los registros de auditoría pueden ser accedidos por personal externo.	

TABLA 1.1