UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÌA EN AUDITORÍA GUBERNAMENTAL

Tema: "LA SEGURIDAD CORPORATIVA COMO EL CONTROL PREVIO DE LA AUDITORÍA FORENSE EN EL SERVICIO DE RENTAS INTERNAS AMBATO DURANTE EL PERÍODO 2010"

Trabajo de Investigación
Previa la obtención del Grado Académico de Magíster en Auditoría Gubernamental

Autora: Mercy Dalila Solis Pazmiño

Director: Eco. Agustín Bombón MBA

Ambato – Ecuador
2011

Al Consejo de Posgrado de la UTA.

El tribunal receptor de la defensa del trabajo de investigación con el tema: "La Seguridad Corporativa como el Control Previo de la Auditoría Forense en el Servicio de Rentas Internas Ambato durante el período 2010", presentado por Mercy Dalila Solis Pazmiño, y conformado por: Dr. Mg. Mauricio Arias P., Dra. Mg. Karina Benítez y Dr. Mg. Marco Espinoza, Miembros del Tribunal, Eco. Agustín Bombón MBA, Director del Trabajo de Investigación y presidido por: Ing. Roberto Ramírez MBA, Presidente del Tribunal; Ing. Juan Garcés Chávez, Director del CEPOS – UTA, una vez escuchada la defensa oral, el Tribunal aprueba y remite el trabajo de investigación para uso y custodia en las bibliotecas de la UTA.

……..
Ing. Roberto Ramírez MBA
Presidente del Tribunal de Defensa

…….
Ing. Mg. Juan Garcés Chávez
DIRECTOR CEPOS

……..
Eco. Agustín Bombón MBA
Director del Trabajo de Investigación

……..
Dr. Mg. Mauricio Arias P.
Miembro del Tribunal

……..
Dra. Mg. Karina Benítez
Miembro del Tribunal

……..
Dr. Mg. Marco Espinoza
Miembro del Tribunal

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de investigación con el tema: "La Seguridad Corporativa como el Control Previo de la Auditoría Forense en el Servicio de Rentas Internas Ambato durante el período 2010", nos corresponde exclusivamente a: Mercy Dalila Solis Pazmiño, Autor y Eco. Agustín Bombón MBA, Director del trabajo de investigación; y el patrimonio intelectual del mismo a la Universidad Técnica de Ambato.

……..	…….
Mercy Dalila Solis Pazmiño	Eco. Agustín Bombón MBA
Autor	Director del Trabajo de Investigación

DERECHOS DE AUTOR

Autorizó a la Universidad Técnica de Ambato, para que haga de este trabajo de investigación o parte de el, un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos de mi trabajo de investigación, con fines de difusión pública, además apruebo la reproducción de esta, dentro de las regulaciones de la Universidad.

……..

Mercy Dalila Solis Pazmiño

Autor

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el tema "La Seguridad Corporativa como el control previo de la Auditoría Forense en el Servicio de Rentas Internas de Ambato durante el período 2010", desarrollado por: Mercy Dalila Solis Pazmiño, egresada de la Maestría de Auditoría Gubernamental, considero que dicho informe investigativo reúne los requisitos y corresponde a las normas establecidas en el Reglamento de Graduación de Postgrado, de la Universidad Técnica de Ambato del Centro de Estudios de Posgrados de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo, para que sea sometido a la evaluación del jurado examinador designado por H. Consejo Directivo.

Ambato, julio del 2011

EL TUTOR

…….

Eco. Agustín Bombón MBA

DEDICATORIA

De una manera especial dedico este trabajo de investigación a Julio, mi esposo, el amor de mi vida, por su apoyo y comprensión y por el impulso que siempre me brinda.

A July y Maty, mis hijos, los pequeños angelitos que Dios me envío, amados seres que me alientan a superarme y demostrarles que todo lo que se propongan pueden cumplirlo.

A mis padres por su formación, por su cariño por todo lo que me han brindado incondicionalmente.

Principalmente a Dios, por la vida, el amor, la salud y las oportunidades que me ha concedido.

AGRADECIMIENTO

Un agradecimiento especial a todas las personas que colaboraron para el desarrollo del presente trabajo investigativo.

Al Servicio de Rentas Internas, Dirección Regional Centro Uno, por toda la apertura y colaboración brindadas.

A los profesores de la Universidad Técnica de Ambato, Facultad de Contabilidad y Auditoría, especialmente a los que prestaron su invalorable contingente en la Maestría de Auditoría Gubernamental, por sus sabios y profesionales conocimientos en la formación no solamente de alumnos sino de seres humanos íntegros.

A mi familia, por su apoyo, confianza y por ser el motivo mayor de mi vida para superarme profesional y personalmente.

Al Economista Agustín Bombón, tutor del presente trabajo de investigación, por su directriz y el apoyo incondicional brindado.

Gracias a todos por su apoyo.

INDICE GENERAL

CONTENIDOS

ÌNDICE DE TABLAS

ÍNDICE DE GRAFICOS

RESUMEN EJECUTIVO

Es relevante considerar que la información constituye un activo que requiere de adecuados controles y seguridades para minimizar los riesgos a los que está expuesta. Si la organización cuenta con un adecuado plan de seguridad corporativa, dispone de un adecuado control previo que sería a su vez un gran apoyo para el desarrollo de una Auditoría Forense.

En el CAPITULO I, se plantea el problema de investigación analizando situaciones críticas que se derivan de insuficientes controles y seguridades, por lo cual se ha contextualizado tomando en cuenta el proceso y entorno de investigación, delimitando la información en el sentido que nos permita cumplir los objetivos planteados tanto generales como específicos.

El marco teórico se desarrolla en el CAPITULO II, fundamentando la orientación filosófica, la que corresponde a la base legal que rige el proceso y control de los activos institucionales, las categorizaciones que sustentan la investigación, en donde se detalla la visión dialéctica y las conceptualizaciones que sustentan las variables de estudio, incluyendo gráficos de inclusión interrelacionados de superordinación y subordinación que nos permiten apreciar de mejor manera el campo de acción del tema planteado. Además se define la hipótesis la cual busca determinar la incidencia de la insuficiente seguridad corporativa en la identificación oportuna de riesgos.

El CAPITULO III, en base al tema planteado nos permite operacionalizar las variables y determinar el enfoque que le damos a la investigación, planteando encuestas y otras técnicas de recolección de información que nos permitirán probar la hipótesis planteada.

Producto de la metodología utilizada, en el CAPÍTULO IV se analizan e interpretan los resultados obtenidos de los cuestionarios aplicados, y de esta manera se procede a la verificación de la hipótesis.

Las conclusiones y recomendaciones se las emite en el CAPÍTULO V del presente trabajo investigativo, espacio en el cual se resume los resultados obtenidos y se sugieren posibles vías de profundización del tema investigado.

En base al tema investigado y a los resultados obtenidos se propone en el CAPÍTULO VI una guía para la implementación de la Seguridad Corporativa, principalmente enfocado a controles previos, recurrentes y posteriores , orientados a convertirse en un sólido sistema para identificar en forma temprana fraudes u otros delitos que atenten a la seguridad de la información (Auditoría Forense).

INTRODUCCIÓN

En la actualidad por el crecimiento de operaciones que realiza el Servicio de Rentas Internas en Ambato, en los diversos departamentos que la integran, ha generado información considerable que requiere un adecuado manejo que garantice su integridad y valor por contener datos de extrema importancia.

Constituyéndose por lo tanto en un activo institucional de incalculable valor, se requiere por ello contar con un plan de seguridad corporativa que abarque todos los aspectos institucionales tanto internos como externos, que permita minimizar los riesgos a los que se encuentra expuesta.

Se hace necesario entonces identificar y administrar los riesgos y evaluar su fortaleza ya que la continuidad de las operaciones, administración y organización de la empresa no debe permanecer en un sistema insuficiente porque podría poner en serio peligro a toda la organización.

El uso de los recursos de la Institución están sujetos a riesgos, lo cual crea la posibilidad de un fácil acceso a información reservada, dando paso a infiltraciones, borrado y un negativo rendimiento que repercute directamente en el logro de los objetivos y metas planteados.

La insuficiente seguridad corporativa puede provocar que los riesgos no sean identificados en forma oportuna y por lo tanto el nivel de acceso a cometer fraudes o delitos de diversa naturaleza, sea muy alto e implique a su vez posibles perjuicios a la Institución.

Diagnosticar la efectividad de aplicación de las Seguridades Corporativas y su nivel de incidencia en el establecimiento de adecuados controles informáticos, que constituyan un eficiente control previo en una Auditoría Forense es el objetivo general del presente proyecto de investigación.

CAPÍTULO I

EL PROBLEMA

1.1. TEMA DE INVESTIGACIÓN

"La Seguridad Corporativa como el control previo de la Auditoría Forense en el Servicio de Rentas Internas Ambato durante el período 2010"

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Contextualización

- **Contexto macro**

El Servicio de Rentas Internas es una Institución Pública creada mediante Ley No.041 del 13 de noviembre de 1997, publicada en el Registro Oficial No. 206 del 2 de Diciembre del mismo año.

La institución está conformada por una Administración Central que trabaja desconcentradamente con ocho Direcciones Regionales que incluyen a su vez Direcciones Provinciales y delegaciones zonales. La Administración Central con jurisdicción en todo el país es la encargada de establecer los lineamientos estratégicos, objetivos, políticas, procesos y procedimientos, así como vigilar su cabal aplicación y cumplimiento.

- **Contexto meso**

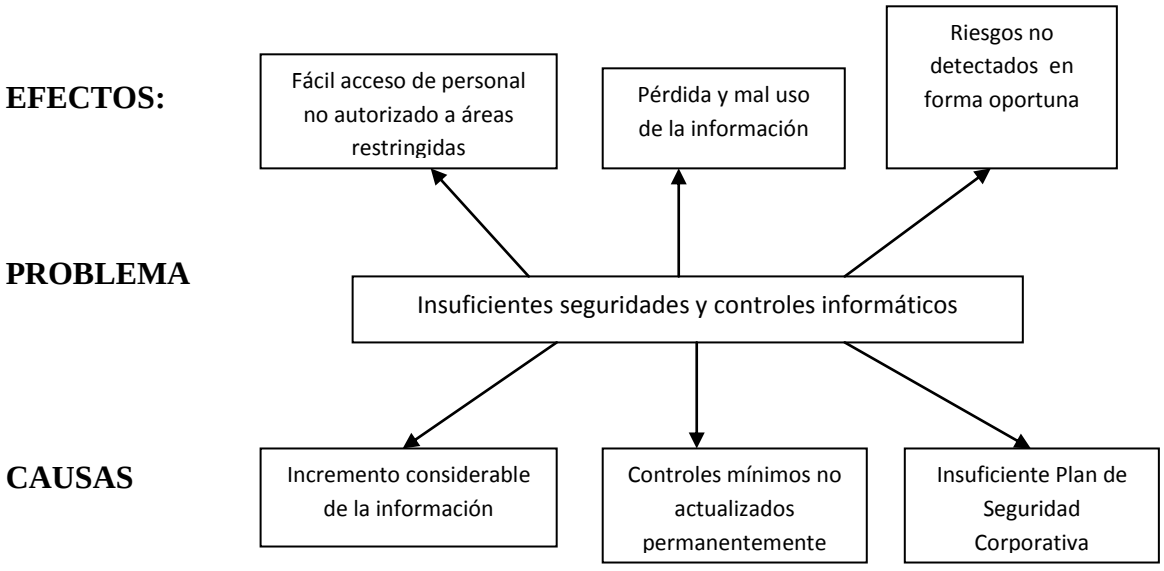
Dentro de la estructura orgánica funcional aprobada por el Directorio de la Institución, la Dirección Regional Centro Uno comprende las provincias de Tungurahua, Cotopaxi y Pastaza, la sede principal es la ciudad de Ambato.
Cuenta con tres agencias zonales: Baños, Agencia Sur (Ambato) y la Maná (Cotopaxi).

- **Contexto micro**

El Servicio de Rentas Internas Ambato, como sede de la Dirección Regional Centro Uno, es responsable de ejecutar los procesos y procedimientos bajo un esquema operativo desconcentrado y uniforme, retroalimentando a la Administración Nacional sobre los sistemas implantados, con el propósito de promover su mejoramiento y alcanzar los objetivos y metas Institucionales, en un marco de eficiencia y productividad.

1.2.2. Análisis Crítico

Gráfico 1: Árbol del Problema



Mediante la ejecución del árbol de problemas, podemos afirmar que la información que administra el Servicio de Rentas Internas Ambato constituye un patrimonio invaluable; su volumen, por los servicios que brinda tanto internos y principalmente externos, es considerable y por ello se requiere fortalecer la seguridad corporativa que ha definido la Institución, para garantizar de manera adecuada y óptima su correcta salvaguarda y custodia, minimizando riesgos de pérdida y uso o accesos no autorizados para beneficio personal que pueden desencadenar en fraudes que afectan gravemente su Imagen Institucional

La mayoría por no decir todos los procesos que se manejan actualmente son automatizados, generando información intangible que requiere de controles informáticos que permitan detectar tempranamente violaciones a políticas, normas o disposiciones legales e internas establecidas

1.2.3. Prognosis

La insuficiente seguridad corporativa puede provocar pérdidas considerables a la Institución especialmente en cuanto a usos no autorizados de información, puede provocar además la difusión errónea de datos, manipulación o inexactitudes, afectando seriamente las operaciones, la toma de decisiones e incluso la imagen.

Las computadoras, servidores y centros de base de datos se han convertido en blanco para fraudes, espionaje, delincuencia y terrorismo informático.

La continuidad de las operaciones, administración y organización de la empresa no debe permanecer en un sistema insuficiente ya que podría poner en serio peligro a toda la organización.

Los riesgos a los que están expuestos los recursos de la Institución, como un fácil acceso a información reservada puede dar paso a infiltraciones, borrado y un negativo rendimiento que repercute directamente en el logro de los objetivos y metas planteados.

1.2.4. Formulación del Problema

¿Es la insuficiente Seguridad Corporativa en el Servicio de Rentas Internas de Ambato causante de débiles controles informáticos, que limitan identificar en forma oportuna los riesgos para el año 2010?

1.2.5. Preguntas Directrices

- ¿Qué produce el incremento considerable para el manejo de información?
- ¿A qué se debe el fácil acceso de personal no autorizado a áreas restringidas?
- ¿Por qué se produce la pérdida y mal uso de la información?
- ¿Por qué los controles existentes no son actualizados permanentemente?

1.2.6. Delimitación

- **Campo:** Ciencias Contables e Informáticas
- **Área:** Auditoría y Sistemas
- **Aspecto:** Auditoría Forense
- **Temporal:** El proyecto de investigación cubrirá el período 2010. El proceso de investigación se desarrollará entre julio 2010 y diciembre de 2010.
- **Espacial:** El Servicio de Rentas Internas se encuentra ubicado, conforme consta en el Registro Único de Contribuyentes, en la Región: Sierra, Provincia: Tungurahua, Cantón: Ambato, calle: Bolívar, Número:15-60 entre Martínez y Lalama (Anexo 1)

1.3. JUSTIFICACIÓN

El creciente y delicado manejo de información que tiene bajo su responsabilidad el Servicio de Rentas Internas Ambato exige contar con mecanismos idóneos y sólidos para precautelar y asegurar el uso correcto para los fines autorizados de las bases de datos que dispone.

Cualquier error puede crear serias dificultades afectando considerablemente la Imagen Institucional.

En la actualidad los conceptos de Auditoría Forense permiten identificar un análisis más exhaustivo de las causas que originan los fraudes en las corporaciones, lo que se denomina control preventivo, y el detectivo que analiza las causas que incentivaron la ejecución de fraudes.

El término Seguridad Corporativa integra un conjunto de sistemas, elementos y recursos que dispone la organización y que están expuestos a diversos riesgos que pueden provocar pérdidas en diversos aspectos.

Trata de establecer mecanismos, planes y otras acciones que minimicen la consecución de delitos especialmente informáticos, y de ahí su relación con Auditoría Forense, que se encarga de establecer los motivos y las causas por las cuales la Institución puede enfrentarse a problemas de seguridad traducidos en fraudes que ocasionan un grave daño no solo económico sino moral.

Es importante garantizar que la información está sujeta a una estricta confidencialidad y aseguramiento que brinde confiabilidad a los contribuyentes de que su información es reservada y confidencial.

El identificar riesgos permite a la Institución definir planes de acción para mitigar las consecuencias de estos riesgos, tenemos un personal mejor preparado para actuar

eficientemente ante contingentes, garantizando un adecuado flujo de la información que no interrumpa el normal desempeño de actividades.

Disponer de una cultura de Seguridad Corporativa brinda garantía y seguridad a usuarios internos y externos, mejora la productividad al identificar posibles procesos sensibles y que requieren por lo tanto atención y controles adecuados.

La auditoría forense es uno de los varios campos de acción que tiene el Contador Público, honesto y altamente capacitado, para desempeñar un rol activo en la lucha contra la corrupción financiera, pública y privada.

El Servicio de Rentas Internas Ambato puede considerarse como una Institución Pública de alto riesgo inherente, por la cantidad de información que administra especialmente, por ello es importante administrar en forma correcta un sistema de Seguridad Corporativa integral, acorde a las últimas actualizaciones tecnológicas basadas en diseños, uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas".

Adicional a este estándar podemos encontrar la ISO 27002, la cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001

1.4. OBJETIVOS

- **Objetivo General**

Diagnosticar la efectividad de aplicación de las Seguridades Corporativas y su nivel de incidencia en el establecimiento de adecuados controles informáticos, que constituyan un eficiente control previo en una Auditoría Forense

- **Objetivos Específicos**

- Evaluar el nivel de aplicación de Seguridades Corporativas que permitan minimizar los factores de riesgo
- Identificar la incidencia de las insuficientes seguridades y controles informáticos en los resultados de Auditoría Forense
- Proponer el diseño de un Sistema Integral de Seguridad Corporativa que constituya un control previo en Auditoría Forense

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES INVESTIGATIVOS

Existen varios estudios sobre Seguridad Corporativa y su relación con diversos tipos de Auditoría como: Financiera, Operacional, Informática, de Gestión y Forense principalmente.

Varias empresas en diferentes países del mundo han desarrollado y aplicado Planes Corporativos de Seguridad, basados en la norma ISO 27002, obteniendo como resultado una gestión integral de la seguridad, basado en el riesgo y gestionado a través de un sistema de control que permite medir la mejora de los niveles de madurez de la Seguridad de la Información

Según lo señala, **Jorge Badillo (2008:4-5)**, en su análisis sobre Administración de Riesgos, tienen éxito sólo aquellas organizaciones que consideran seriamente los riesgos y toman pasos proactivos para crear un ambiente apropiado para reducir su ocurrencia Por otra parte analicemos el término "forense" que proviene del latín "forensis" que significa "público y manifiesto" o "perteneciente al foro"; a su vez "forensis" se deriva de "fórum" que significa "foro", "plaza pública"

La Auditoría Forense comprende a la Auditoría Forense Preventiva y la Auditoría Forense Detectiva. De acuerdo al enfoque del proyecto de investigación nos basaremos en la definición de Auditoría Forense Preventiva, que según define **Jorge Badillo (2008: 24-25)**, en el artículo publicado sobre el tema de referencia, la Auditoría Forense Preventiva está orientada a proporcionar aseguramiento (evaluación) o asesoría a las organizaciones respecto de su capacidad para disuadir, evitar, detectar y reaccionar ante fraudes financieros, pudiendo incluir trabajos de consultoría para implementar programas y controles anti-fraude; esquemas de alerta temprana de irregularidades; sistemas de administración de denuncias.

Este enfoque es proactivo por cuanto implica tomar decisiones y acciones en el presente para evitar fraudes en el futuro.

En todo caso al asociar la auditoría forense preventiva con la detectiva obtenemos una Auditoría Forense Integral.

Una sólida estructura de Seguridad Corporativa constituye un control interno adecuado y permite minimizar riesgos de cualquier naturaleza, y su efectividad se mide con los resultados de ejecución de una Auditoría Forense Integral.

Dentro del Control Interno, **Mario Andrade (2006: 2)**, menciona respecto de la Gestión de Riesgos Corporativos, que siempre se busca promover la adopción de estrategias que permitan el logro de los objetivos institucionales y de todos los niveles de la organización en un ambiente de transparencia y honestidad.

Dentro de la evaluación de riesgos se revisará por parte de los auditores interesados la identificación de eventos, evaluación de riesgos, la respuesta a los riesgos y las actividades de control adoptados, si no se toman las acciones preventivas correspondientes podría verse seriamente afectada la gestión institucional.

Según **Miltón Maldonado (2003: 12)**, hay diferentes motivos para el fraude, identificando elementos como las causas por las cuales las personas lo hacen, la oportunidad, la decisión, el acto en sí, el sujeto y el efecto.

Un sistema débil de control interno reflejado en la poca seguridad corporativa provoca una oportunidad a quien es propenso a cometer irregularidades de cualquier tipo.

2.2. FUNDAMENTACIÓN FILOSÓFICA

El presente proyecto de investigación será predominantemente cualitativo, por cuanto la Seguridad Corporativa afecta a los individuos e Institución bajo lo cual se trata de solucionar los problemas con ayuda de los técnicos en la materia

Según información presentada por **Roberto Hernández y otros (2003: 4-6),** indica que el enfoque cualitativo, tiene su origen con Max Weber, quien reconoció que la medición y descripción de variables sociales deben considerar los significados subjetivos y el entendimiento del contexto donde ocurre un fenómeno.

El enfoque cualitativo, por lo común, se utiliza primero para descubrir y refinar preguntas de investigación, para probar hipótesis; su propósito consiste en "reconstruir" la realidad, tal y como la observan los actores de un sistema social previamente definido. A menudo se llama "holístico" porque se precia de considerar el todo, sin reducirlo al estudio de sus partes

Tomando como referencia a **Víctor Hugo Abril (2008: 5),** indica que la Investigación Cualitativa se ha concebido últimamente como aquel tipo de investigación en el cual participan los individuos y comunidad para solucionar sus propias necesidades y problemas, bajo la guía de técnicos al respecto, pero con la participación directa de todos los interesados en su desarrollo.

Por lo expuesto la presente investigación se fundamenta entonces en el paradigma positivista, el mismo que según lo define **Luis G. Meza C. (2010: Internet)**, el positivismo es una corriente de pensamiento cuyos inicios se suele atribuir a los planteamientos de Auguste Comte, y que no admite como válidos otros conocimientos sino los que proceden de las ciencias empíricas

La Investigación Cualitativa no sólo no provee de los medios para explorar situaciones complejas y caóticas de la vida real, sino que nos aportan múltiples opciones metodológicas sobre cómo acercarse a tal ámbito de acuerdo con el problema y los objetivos del estudio, además la recogida, análisis e interpretación de datos que no son objetivamente mensurables

La investigación cualitativa en el presente proyecto pretende comprender las complejas relaciones entre todo lo que existe, además consiste en descripciones detalladas de situaciones, eventos, personas, interacciones y comportamientos que son observables. Incorpora lo que los participantes dicen, sus experiencias, actitudes, creencias, pensamientos y reflexiones tal como son expresadas por ellos mismos y no como uno los describe

2.3. FUNDAMENTACIÓN LEGAL

- La Constitución de la República del Ecuador, aprobada en referéndum el 28 de septiembre de 2008 y publicada en el Registro Oficial 449 del 20 de octubre de 2008, en su artículo 211 dispone que le compete a la Contraloría General del Estado realizar el control de la utilización de los recursos estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que disponen de recursos públicos

- La Ley Orgánica de la Contraloría General del Estado expedida mediante Ley 73 y publicada en el Registro Oficial Suplemento 595 de 12 de Junio del 2002, en la parte pertinente señala: "Art. 4.- Régimen de control de las personas

jurídicas con participación estatal.- Para todos los efectos contemplados en esta Ley, están sometidas al control de la Contraloría General del Estado, las personas jurídicas y entidades de derecho privado, exclusivamente sobre los bienes, rentas u otras subvenciones de carácter público de que dispongan, cualesquiera sea su monto, de conformidad con lo dispuesto en el inciso segundo del artículo 211 de la Constitución Política de la República"

En el mismo cuerpo legal el Art. 6, señala: "Componentes del Sistema.- La ejecución del sistema de control, fiscalización y auditoría del Estado se realizará por medio de:

1.- El control interno, que es de responsabilidad administrativa de cada una de las instituciones del Estado a las que se refiere el artículo 2 de esta Ley; y,

2.- El control externo que comprende:

a) El que compete a la Contraloría General del Estado; y,
b) El que ejerzan otras instituciones de control del Estado en el ámbito de sus competencias"

El Art. 9 en la parte pertinente señala, " Concepto y elementos del Control Interno.- El control interno constituye un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales. Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, los riesgos institucionales en el logro de tales objetivos y las medidas adoptadas para afrontarlos, el sistema de información, el cumplimiento de las normas jurídicas y técnicas; y, la corrección oportuna de las deficiencias de control.

El control interno será responsabilidad de cada institución del Estado, y tendrá como finalidad primordial crear las condiciones para el ejercicio del control externo a cargo de la Contraloría General del Estado.

Además la Ley Orgánica de la Contraloría en el Art. 12 indica: "Tiempos de control.- El ejercicio del control interno se aplicará en forma previa, continua y posterior:

a) Control previo.- Los servidores de la institución, analizarán las actividades institucionales propuestas, antes de su autorización o ejecución, respecto a su legalidad, veracidad, conveniencia, oportunidad, pertinencia y conformidad con los planes y presupuestos institucionales;

b) Control continuo.- Los servidores de la institución, en forma continua inspeccionarán y constatarán la oportunidad, calidad y cantidad de obras, bienes y servicios que se recibieren o prestaren de conformidad con la ley, los términos contractuales y las autorizaciones respectivas"

- La Ley de Creación del Servicio de Rentas Internas, creada mediante Ley No.41 publicada en el Registro Oficial 206 del 2 de diciembre de 1997, que en el artículo 1 dispone que: "..Créase el Servicio de Rentas Internas (SRI) como una entidad técnica y autónoma, con personería jurídica, de derecho público, patrimonio y fondos propios, jurisdicción nacional y sede principal en la ciudad de Quito. Su gestión estará sujeta a las disposiciones de esta Ley, del Código Tributario, de la Ley de Régimen Tributario Interno y de las demás leyes y reglamentos que fueren aplicables y su autonomía concierne a los órdenes administrativo, financiero y operativo"

  El mismo cuerpo legal en el artículo 17 señala: "Del control interno.- El Servicio de Rentas Internas establecerá los métodos y procedimientos propios de control interno, de conformidad con lo previsto en la Ley Orgánica de Administración Financiera y Control.

Se establecerá la Unidad de Auditoría Interna que efectuará el examen posterior de las operaciones financieras y administrativas de la entidad y presentará sus informes para conocimiento del Director General del Servicio de Rentas Internas, Directorio y Contralor General del Estado"

- Código de Ética, expedido mediante resolución general NAC-DGER2007-1350 el 29 de diciembre de 2007 y publicada en el Registro Oficial No.253 de 16 de enero de 2008, que busca consolidar un comportamiento moral y compromiso de todos los funcionarios, definido así en los artículos 4: "Compromiso personal de los servidores: Los servidores de la Administración Tributaria deben asumir la responsabilidad personal de conocer y promover el cumplimiento de los principios, valores y pautas contenidos en este Código, el cual será un referente para el fortalecimiento institucional y la promoción de la ética, al interior del SRI"

El artículo 15, respecto de la utilización de los bienes y recursos públicos, indica: "Uso de bienes y recursos públicos.- Los servidores del SRI utilizarán los bienes y recursos públicos institucionales, únicamente para actividades relacionadas con el desarrollo de actividades inherentes a la Administración Tributaria.

En el mismo código de ética el artículo 19, señala: "Uso de información para fines permitidos.- Es obligación del servidor utilizar la información a la que tiene acceso en razón de su trabajo, únicamente para los fines permitidos, conforme a la normativa y a las ordenes del servidor competente. De igual forma es deber del servidor abstenerse de acceder a la información que no le haya sido autorizada, asignada o permitida…"

El artículo 20 señala respecto de las políticas de uso de claves: "Cada servidor tendrá especial cuidado, uso y manejo de las claves y seguridades empleadas para acceder a la red de información electrónica institucional…"

Finalmente el artículo 22 se refiere a la prevención de revelación no autorizada, señalando que "El custodio de la información, debe realizar los esfuerzos necesarios para precautelar la seguridad y prevenir la revelación no autorizada de información del SRI" y el artículo 23 que indica sobre el uso de la información tributaria: "Los servidores no podrán revelar información tributaria referente a los contribuyentes, a servidores no autorizados…"

- Acuerdo de Confidencialidad sobre Manejo de Información, asumido por todos los integrantes de la Organización, y regularizado mediante resolución general NAC-DGER2008-0987 del 7 de mayo de 2008.

2.4. CATEGORÍAS FUNDAMENTALES

2.4.1 Visión dialéctica de conceptualizaciones que sustentan las variables del problema

2.4.1.1. Marco conceptual variable independiente

Se requiere fortalecer la seguridad corporativa que ha definido la Institución, para garantizar de manera adecuada y óptima su correcta salvaguarda y custodia, minimizando riesgos de pérdida y uso o accesos no autorizados para beneficio personal que pueden desencadenar en fraudes que afectan gravemente su Imagen Institucional

La palabra Seguridad en su sentido más básico se refiere a la ausencia de riesgos en todos los ámbitos.

Acorde con esta definición y la evolución en el transcurso del tiempo, el término seguridad ha adquirido mayor relevancia, además ha sufrido transformaciones teórico como prácticas, a tal punto que en la actualidad no existe ninguna

actividad desarrollada por el ser humano en el que no se requiera contar con seguridades para minimizar riesgos de cualquier naturaleza.

Dentro del ámbito de la Administración Pública se han establecido y evolucionado diversos tipos de control encaminados a precautelar principalmente la integridad física del recurso humano y material, cumpliendo con la normativa legal aplicable para minimizar riesgos que afecten gravemente la integridad de sus recursos disponibles y por lo tanto evitar sanciones.

Debido a una serie de problemas identificados en el Gobierno de los Estados Unidos de América, empezando con el caso Watergate en la década de los 70 y llegando a las dificultades financieras del Sistema de Ahorro y Crédito en la década de los 80, la Comisión del Senado de los EUA, Treadway Comission gestionó la formación del "Commitee of Sponsoring Organizations" (Comité de Organizaciones Patrocinadoras), conocido por sus siglas en inglés como COSO.

Este Comité realizó una investigación sobre el conocimiento, aplicación y mejora de los criterios de control interno en las grandes corporaciones, las medianas y pequeñas empresas, incluyendo temas relacionados con el mejoramiento técnico y el alcance de las funciones de diseño, implantación y evaluación de los controles internos integrados de las organizaciones.

En septiembre de 1992 se publicó la versión en inglés denominado "Informe COSO". COSO contó con la asistencia técnica permanente de la firma Coopers & Lybrand para la investigación.

Otros organismos profesionales de los países industrializados han definido su enfoque sobre el control interno, basados en los criterios definidos en el Informe COSO.

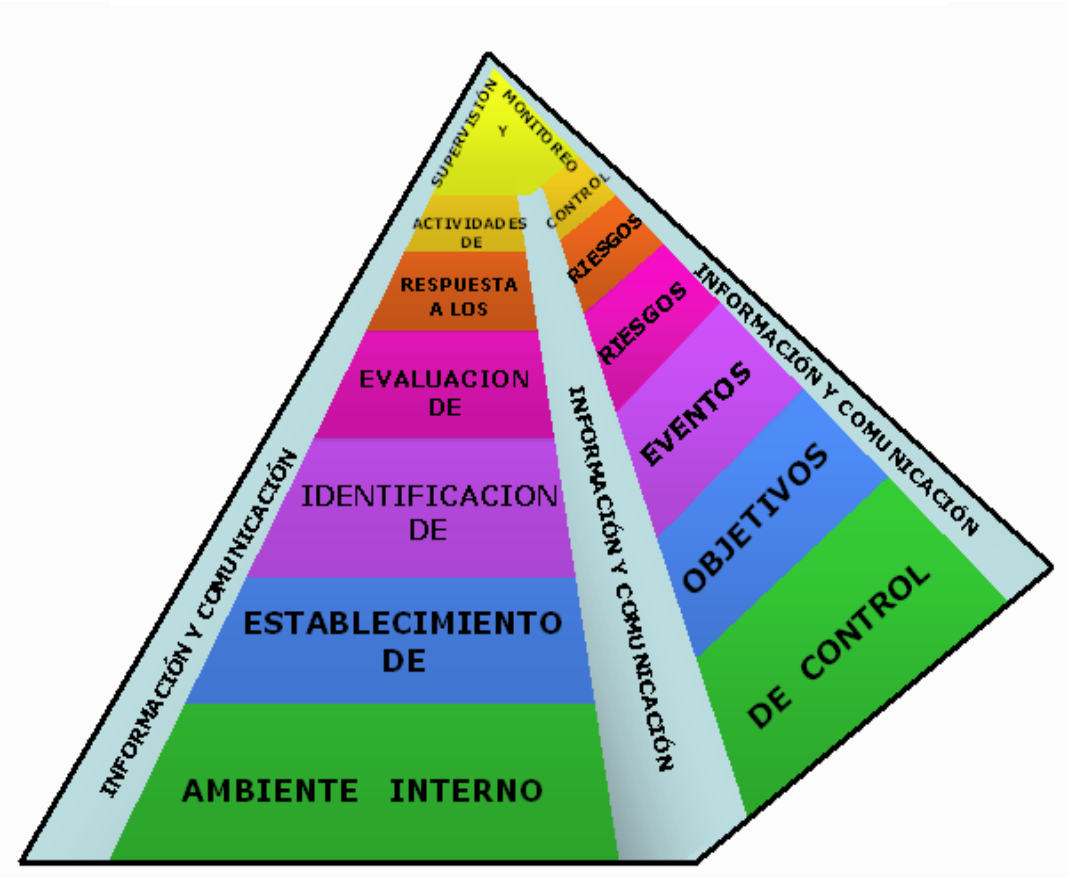
En el informe COSO, el control interno se define como un proceso, efectuado por el consejo de administración, la dirección y el resto de personal de una entidad (todos), diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia en las operaciones (OPERACIONES).
- Fiabilidad de la información financiera (y de gestión) (REPORTES FINANCIEROS).
- Cumplimiento de las leyes y normas aplicables (CUMPLIMIENTO).
- Salvaguarda de los recursos de la entidad

Toda organización, independientemente de la actividad o del sector al que pertenezca, requiere definir y desarrollar los siguientes componentes en el marco integrado de control interno:

1. Ambiente de Control (y Trabajo),
2. Evaluación de Riesgos,
3. Actividades de Control,
4. Información y Comunicación (Sistemas de); y,
5. Supervisión (Monitoreo).

Gráfico 2: Componentes de control interno



Los cinco componentes incorporados en la pirámide de control interno permiten observar de manera objetiva la relación existente entre cada uno de ellos, cuando el segmento asignado a cada uno se junta con otro u otros componentes y la manera como la debilidad o la ausencia de uno de ellos, promueve el desarrollo o facilita el deterioro del conjunto.

Los componentes de control interno presentan un esquema que partiendo del ambiente de control como la parte más amplia de la pirámide auspicia el funcionamiento efectivo de los cuatro componentes (evaluación de riesgo, actividades de control, información y comunicación y supervisión) que se asientan sobre él, llegando hasta el final y asegurando su funcionamiento en todos los

niveles de la organización. El componente información y comunicación es el más dinámico y permite su interrelación desde la base de la pirámide (ambiente de control) hasta la cúspide (supervisión). Mediante los reportes procesados para los diferentes niveles y en varias instancias; regresa a la base de la pirámide a través de la comunicación que se procesa desde la supervisión hacia los tres componentes y así completar el proceso al llegar a la base de pirámide.

Marco Integrado de Control Interno Latinoamericano.- MICIL

En la Conferencia Interamericana de Contabilidad de San Juan, Puerto Rico en 1999 se recomendó un marco latinoamericano de control similar al COSO en español en base de las realidades de la región. Se nombró una comisión especial de representantes de la Asociación Interamericana de Contabilidad (AIC) y la Federación Latinoamericano de Auditores Interno (FLAI) para iniciar el desarrollo de tal marco. En el año 2000, el Proyecto Responsabilidad/Anticorrupción en las Américas (Proyecto AAA), financiado por la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) y administrado por Casals & Associates, Inc. (C&A), reconoció la necesidad de contar con un modelo que sirviera de marco de control interno para las empresas y los gobiernos de la región de América Latina.

Luego de diversas consultas con funcionarios gubernamentales responsables de la administración financiera en Latinoamérica, líderes empresariales y funcionarios de USAID en la región y en Washington, DC, el Proyecto AAA se comprometió a apoyar el desarrollo de dicho marco.

El Marco Integrado de Control Interno para Latinoamérica (MICIL) -resultado de dicho esfuerzo- es un modelo basado en estándares de control interno para las pequeñas, medianas y grandes empresas desarrolladas por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (Committee of Sponsoring Organizations of the Treadway Commission-COSO).

En la preparación del MICIL, expertos trabajaron conjuntamente con los líderes de asociaciones profesionales comprometidas en la mejora de la rendición de cuentas y la transparencia; en particular la Federación Latinoamericana de Auditores Internos (FLAI) y la Comisión Interamericana de Auditoría Interna de la Asociación Interamericana de Contabilidad (AIC).

Las dos últimas décadas, a partir de los años 80, han sido perjudiciales para los países de América Latina y las organizaciones que la integran. Los resultados macroeconómicos y del desarrollo alcanzado son muy pobres. Las diferencias económicas entre los ricos y los pobres son cada vez mayores; mientras los primeros lo tienen todo, los segundos carecen de recursos para su alimentación y la satisfacción de sus necesidades básicas. En general, se manifiesta que el 43% de la población en América Latina vive en condiciones de pobreza.

Estos desequilibrios se fundamentan en los modelos utilizados por los países para programar, ejecutar sus actividades y promover su desarrollo. Ante tal necesidad, también se ha requerido introducir reformas políticas para permitir la participación activa de todos sus ciudadanos. Estos procesos, consecuentemente, requieren ajustes fundamentales en el diseño y aplicación de herramientas como son los controles internos. Los conceptos modernos de control interno tienen absoluta consistencia con los ajustes estructurales de nuestros países.

El Marco Integrado de Control Interno Latinoamericano (MICIL) puede enfocarse a escala global y específica. A escala global: hacia los poderes de un Estado, a los sectores importantes de la economía, a las entidades públicas específicas, a las diferentes actividades de las empresas privadas, a las organizaciones de la sociedad civil y a las municipalidades. A escala específica: puede ser enfocado hacia las unidades de operación y/o a las principales actividades consideradas en el modelo genérico de organización.

Las dificultades por las cuales están pasando las finanzas y el crecimiento sostenible, tanto de los países, como de las corporaciones, las empresas privadas, las instituciones públicas, las municipalidades y las organizaciones de la sociedad civil; en muchos de los casos, se deben a situaciones que pueden ser prevenidas mediante un marco integrado de control interno diseñado, implantado y aplicado formalmente.

Prevención que también involucra la creación de una cultura, en la que cuando al menos una persona de las que participan en el proceso, cumpla con la responsabilidad social de sus funciones y haga evidente las situaciones erradas o irregulares, en principio, a la autoridad adecuada en la estructura de la organización; y, de ser necesario, ante los organismos de la sociedad en general.

Algunas corporaciones y empresas importantes tienen en funcionamiento un Comité de Ética y Transparencia o corresponden a otras denominaciones, en el que se conocen y resuelven los problemas importantes, que podrían presentar dificultades por violar las normas y los valores bajo los que opera la organización.

Los problemas, calificándolos de una manera positiva, que se han suscitado en los últimos años en la administración de las grandes corporaciones de los países industrializados demuestran, que la situación se está generalizando, debido a la competencia y la necesidad de presentar resultados contables positivos.

Es evidente que, los mayores problemas se ubican en los niveles superiores de las organizaciones, incluyendo a los organismos de vigilancia, supervisión y seguimiento del gobierno. Problemas como los que se mencionan en los párrafos siguientes, no están ausentes en las empresas que tienen acceso a la información financiera y de gestión de las corporaciones que cotizan en la Bolsa de Valores y cuyas acciones están disponibles al público para invertir. Gran parte de esta situación se debe a las debilidades en la aplicación de los criterios de control

interno, en la toma de decisiones por los niveles superiores, en su aceptación por los niveles gerenciales y al formalizarlas en los niveles operativos.

Es poco conocido el marco integrado de control interno en las entidades públicas, las empresas privadas y el propio Estado. El conocimiento, análisis y difusión de las características y cualidades del control interno han estado relacionadas con el conocimiento y estudio de pocas disciplinas y, con un enfoque restringido a los asuntos financieros y administrativos, a pesar de la necesidad de conocer sobre un ambiente de control sólido, como base para el funcionamiento de las organizaciones, los valores, la ética y la transparencia como su cimiento.

En el ámbito internacional, existen varios casos con problemas que han presentado pérdidas importantes para los inversionistas públicos, el cierre, la quiebra o liquidación de importantes empresas.

La mayoría de ellos, han identificado como la causa principal del problema a los métodos de registro contable utilizados, el mismo que hace visible sólo el efecto de las decisiones tomadas en los niveles superiores de los organismos públicos y privados.

La razón o las causas fundamentales están contenidas en el marco integrado del control interno que incluye el ambiente de control de la entidad y dentro de este las disposiciones legales y reglamentarias bajo las cuales opera, así como los valores, la ética y la transparencia con la que opera, a su interior y hacia el exterior.

Diversos autores han identificado e incluso establecido varias clasificaciones de riesgos, pero antes de analizar cada uno de ellos y especialmente los relativos a nuestra investigación, conozcamos primero que es un riesgo.

El término Seguridad Corporativa integra un conjunto de sistemas, elementos y recursos que dispone la organización y que están expuestos a diversos riesgos que pueden provocar pérdidas en diversos aspectos. Trata de establecer mecanismos, planes y otras acciones que minimicen la consecución de delitos especialmente informáticos, y de ahí su relación con Auditoría Forense, que se encarga de establecer los motivos y las causas por las cuales la Institución puede enfrentarse a problemas de seguridad traducidos en fraudes que ocasionan un grave daño no solo económico sino moral.

Definamos el término riesgo, que según **Alberto Chiriboga (2008: 145)**, en su diccionario técnico financiero define el riesgo como un evento de cualquier naturaleza cuya ocurrencia puede afectar la capacidad del cliente para hacer frente a sus obligaciones. El riesgo normal es el valor esperado de pérdida. El riesgo potencial es el porcentaje de pérdida esperada o de recuperación no total.

En su análisis sobre Administración de Riesgos, **Jorge Badillo (2008: 9)**, define al riesgo como cualquier asunto que podría evitar alcanzar los objetivos, en el sentido más amplio es la exposición a la adversidad. El riesgo se mide en términos de consecuencia y probabilidad.

Dentro de una interpretación académica el riesgo es una medida de incertidumbre que involucra el logro de los objetivos institucionales, lo que incluye las consecuencias y probabilidad de que un evento negativo ocurra

Los tipos de riesgos pueden ser: inherente y residual, el inherente es el riesgo para la entidad en ausencia de cualquier acción realizada por la administración para alterar la probabilidad e impacto. El riesgo residual es el riesgo remanente después de la acción realizada por la administración para alterar su probabilidad e impacto.

Es importante conocer el concepto de control, según **Jorge Badillo (2008: 10)**, el control es cualquier cosa que se haga para manejar riesgos de fracaso en la obtención de objetivos corporativos, aquí entra la Seguridad Corporativa como un plan de control para minimizar riesgos que permitan ejercer un control para la consecución de los objetivos institucionales.

Por el avance tecnológico la Seguridad Corporativa cuenta hoy con sistemas de información acorde a las últimas actualizaciones tecnológicas basadas en diseños, uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001

Según **Wikipedia (2010: Internet)**, COBIT (Objetivos de Control de la Tecnologías de la Información) tiene como misión investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores." Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

Otro de los conceptos que ha tomado fuerza en la actualidad es la implementación de ISO 27001 y 27002, al respecto el **Forum Spain (2010: Internet)**, señala que

la información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización.

El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

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

La ISO 27002:2005, considera los siguientes aspectos: Introducción, conceptos generales de seguridad de la información y SGSI. Campo de aplicación: se especifica el objetivo de la norma. Términos y definiciones: breve descripción de los términos más usados en la norma. Estructura del estándar: descripción de la estructura de la norma. Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información. Política de seguridad: documento de política de seguridad y su gestión. Aspectos organizativos de la seguridad de la información: organización interna; terceros. Gestión de activos: responsabilidad sobre los activos; clasificación de la información. Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo. Seguridad física y ambiental: áreas seguras; seguridad de los equipos. Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema;

protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión. Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo. Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.

Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio. Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

En fin sobre seguridad y con el avance tecnológico las Instituciones encuentran un punto de apoyo sólido para la tarea de asegurar activos y minimizar riesgos potenciales incluidos los fraudes corporativos, en donde interviene la Auditoría Forense.

2.4.1.2. Marco conceptual variable dependiente

Dentro del marco conceptual de la variable dependiente, comenzaremos exponiendo la definición de Auditoría, que según **Walter Kell y otros (1983: 25)**

indica que es un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados.

Dentro de Auditoría podemos encontrar varias clasificaciones de diversos autores y enfocada a diversos aspectos, sin embargo consideramos apropiada la clasificación que realiza **Miltón Maldonado (2003: 17)** en su libro sobre Auditoría Forense, indica que existen la Auditoría Financiera, cuyo propósito es formular y expresar una opinión sobre la razonabilidad de los estados financieros de una entidad, la Auditoría de Gestión que busca evaluar la eficiencia, efectividad y economía con la que se manejan los recursos de una entidad, un programa o actividad; el cumplimiento de las normas éticas por el personal y la protección del medio ambiente.

La Auditoría Tributaria que busca verificar y controlar el pago de las obligaciones tributarias de acuerdo a la Ley. La Auditoría Gubernamental que reúne conceptos de la Auditoría Financiera, de Gestión y Forense incorporando el control de legalidad. La Auditoría Forense busca prevenir e investigar presuntos hechos de corrupción.

Como podemos ver del concepto de Auditoría Forense y Auditoría Gubernamental existe una estrecha relación entre ambas, con un factor común que las complementan y es el enfoque del presente proyecto de investigación buscar la prevención de fraudes con estricto apego al principio de legalidad.

Es importante para este propósito evaluar el sistema de control interno pero para ello conozcamos el concepto de control interno que **Mario Andrade (2006: 5)**, nos indica que es un proceso efectuado por el consejo de administración, la dirección y el resto de personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de

objetivos dentro de las siguientes categorías: honestidad y responsabilidad, eficacia y eficiencia en las operaciones, fiabilidad de la información, salvaguarda de los recursos y cumplimiento de leyes y normas.

La seguridad, en un amplio sentido, constituye el conjunto de normas preventivas y operativas, con apoyo de procedimientos, programas, sistemas, y equipos de seguridad y protección, orientados a neutralizar, minimizar y controlar los efectos de actos ilícitos o situaciones de emergencia, que afecten y lesionen a las personas y los bienes que estas poseen

Los riesgos se definen como una exposición a la adversidad frente a un resultado deseado o esperado, es decir aquello que impida lograr los objetivos planteados.

El riesgo se mide en términos de consecuencias y probabilidad. El riesgo es por sí mismo una condición de la existencia, es inherente a cualquier recurso o actividad; por ello el riesgo no se crea ni se destruye; solo se transforma.

El control implica cualquier cosa que se haga para manejar riesgos de fracaso en la obtención de objetivos corporativos.

La auditoría forense es uno de los varios campos de acción que tiene el Contador Público, honesto y altamente capacitado, para desempeñar un rol activo en la lucha contra la corrupción financiera, pública y privada.

Al referirnos a Auditorías Fiscales, según lo indica **John Willingham (1982: 13)**, el gobierno es una gran empresa; hay una cantidad de oficinas responsables de la administración de regulaciones complejas.

Se requiere entonces de un adecuado manejo y cuidado de la información que genera y por la delicadeza de la información que tiene a su cargo debe contar con adecuados mecanismos de salvaguarda.

Un papel muy importante dentro del control y eficiente manejo de recursos públicos tiene la Unidad de Auditoría Interna, **Jorge Lozano (1973: 15)**, indica que la Auditoría Interna nació con la necesidad de certificar o comprobar que las cifras de los reportes internos eran correctas. En la actualidad son los mejores usuarios de Seguridad Corporativa porque constituye un soporte para la ejecución y cumplimiento de su trabajo, vigilar que la administración adopte adecuados mecanismos de control.

En la obra de **Blanco Yanel (1987: 16)**, se señala que el alcance del trabajo del revisor fiscal es más amplio que el del auditor externo, porque la revisoría fiscal no se limita exclusivamente al examen de las cuentas con el propósito de emitir una opinión sobre la razonabilidad de las mismas sino que se extiende a la vigilancia y control de los actos cumplidos por los administradores y velar por un adecuado control interno.

De ahí la responsabilidad de las Instituciones de administrar un adecuado sistema de seguridad que brinde tranquilidad sobre prevención, detección y acciones para cuidar los recursos a ellas asignados.

La auditoría y la seguridad corporativa están estrechamente ligadas y la segunda se convierte en el paso previo, en el control interno de la segunda para detener y no permitir acciones que perjudiquen a la organización. La información generada por una organización, en cualquiera de sus formas, constituye un activo de incalculable valor por ello, ningún esfuerzo será en vano para precautelar, prevenir y promover su adecuado uso, custodia y respeto que se verán reflejados en el logro de objetivos estratégicos propuestos en su planificación.

Auditoría Forense.

Cuando en la ejecución de labores de auditoría (financiera, de gestión, informática, tributaria, ambiental, gubernamental) se detecten fraudes financieros

significativos; y, se deba (obligatorio) o desee (opcional) profundizar sobre ellos se está incursionando en la denominada auditoría forense. La investigación será obligatoria dependiendo de: 1) el tipo de fraude; 2) el entorno en el que fue cometido; y, 3) la legislación aplicable. La labor de auditoría forense también puede iniciar directamente sin necesidad de una auditoría previa de otra clase, por ejemplo en el caso de existir denuncias específicas.

La auditoría forense es aquella labor de auditoría que se enfoca en la prevención y detección del fraude financiero; por ello, generalmente los resultados del trabajo del auditor forense son puestos a consideración de la justicia, que se encargará de analizar, juzgar y sentenciar los delitos cometidos (corrupción financiera, pública o privada).

En su libro de "Auditoria Forense", **Milton Maldonado (2003: 9)**, señala lo siguiente:

"La AUDITORIA FORENSE es el otro lado de la medalla de la labor del auditor, en procura de prevenir y estudiar hechos de corrupción. Como la mayoría de los resultados del Auditor van a conocimiento de los jueces (especialmente penales), es usual el término forense. (...) Como es muy extensa la lista de hechos de corrupción conviene señalar que la Auditoría Forense, para profesionales con formación de Contador Público, debe orientarse a la investigación de actos dolosos en el nivel financiero de una empresa, el gobierno o cualquier organización que maneje recursos."

Según **Miguel Cano y Danilo Lugo (2005: 16, 20)**, en su libro "Auditoría Forense en la Investigación Criminal del Lavado de Dinero y Activos" presentan la siguiente definición:

"(...) se define inicialmente a la auditoría forense como una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas y privadas, (...).

(...) la auditoría forense es, en términos contables, la ciencia que permite reunir y presentar información financiera, contable, legal, administrativa e impositiva, para que sea aceptada por una corte o un juez en contra de los perpetradores de un crimen económico, (...)."

"La Auditoría Financiera Forense es relativamente nueva pero cada vez más importante. (...). A raíz de la globalización se ha acentuado también el fenómeno de la corrupción, especialmente en la alta dirección ("crimen de cuello blanco"), con estructuras tan complejas como las utilizadas para el lavado de activos en sus diversas modalidades. (...). El análisis de ello ha conducido a ver la auditoría financiera con otra perspectiva: los supuestos de empresa en marcha y buena fe, que conducen a la detección de irregularidades, hacen crisis frente a estos nuevos delitos.

En sus inicios, la auditoría forense surge con los intentos por detectar y corregir el fraude en los estados financieros. Posteriormente ha ido ampliando su campo de acción en la medida que ha desarrollado técnicas específicas para combatir el crimen y trabaja estrechamente en la aplicación de la justicia.

Parte, entonces, del supuesto de que no hay empresa (lo cual hace extremadamente difícil la detección del crimen) y que la intención es el dolo. Por lo tanto, se requiere aplicar un conjunto completamente nuevo de técnicas para detección y análisis de la corrupción.

El problema de la prueba (en general), como lo indica **Alberto Mantilla (2004: 708)**, así como de la evidencia (de auditoría) adquieren una dimensión completamente nueva dado que son útiles en la medida que pueden ser aceptadas en los estrados judiciales."

Pablo Fudim (2011: Internet), define a la auditoría forense de la siguiente manera: "La auditoria forense es la rama de la auditoria que se orienta a participar en la investigación de ilícitos.

La auditoria forense procede dentro del contexto de un conflicto real o de una acción legal con una pérdida financiera significativa, donde el auditor forense ofrece sus servicios basados en la aplicación del conocimiento relacionado con los dominios de lo contable (como información financiera, contabilidad, finanzas, auditoría y control) y del conocimiento relacionado con Investigación financiera, cuantificación de pérdidas y ciertos aspectos de ley.

Un compromiso de auditoría forense involucra por lo menos: análisis, cuantificación de pérdidas, investigaciones, recolección de evidencia, mediación, arbitramento y testimonio como un testigo experto.

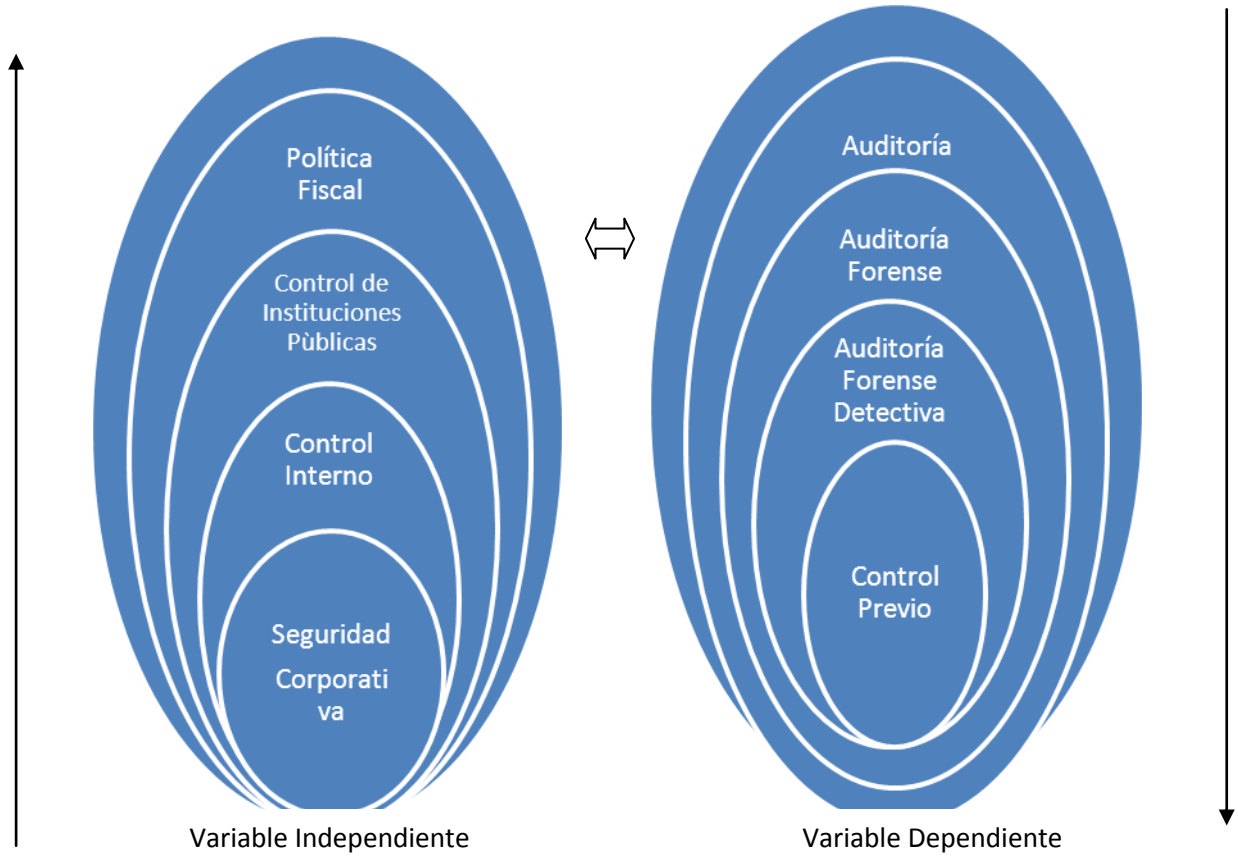
Cuando se actúa en calidad de auditores forenses dentro de una investigación, se pone en práctica toda la experiencia en contabilidad, auditoria e investigación. Como también la capacidad del auditor para transmitir información financiera en forma clara y concisa ante un tribunal.

Los auditores forenses están entrenados para investigar más allá de las cifras presentadas y manejar la realidad comercial del momento".

2.4.2 Gráficos de Inclusión interrelacionados

2.4.2.1. Superordinación conceptual

Gráfico 3: Superordinación conceptual



2.4.2.2. Subordinación conceptual

Gráfico 4: Variable Independiente

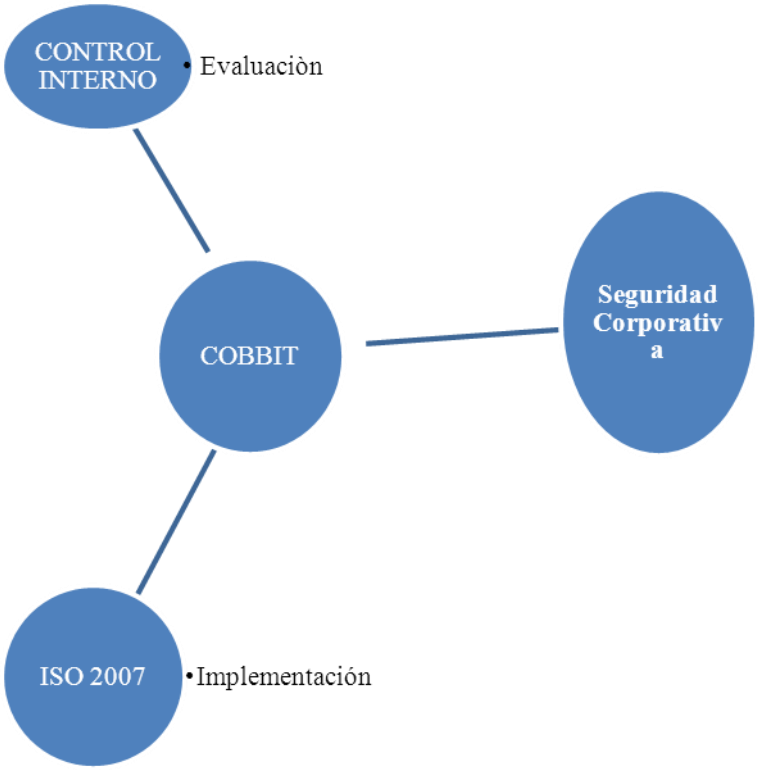
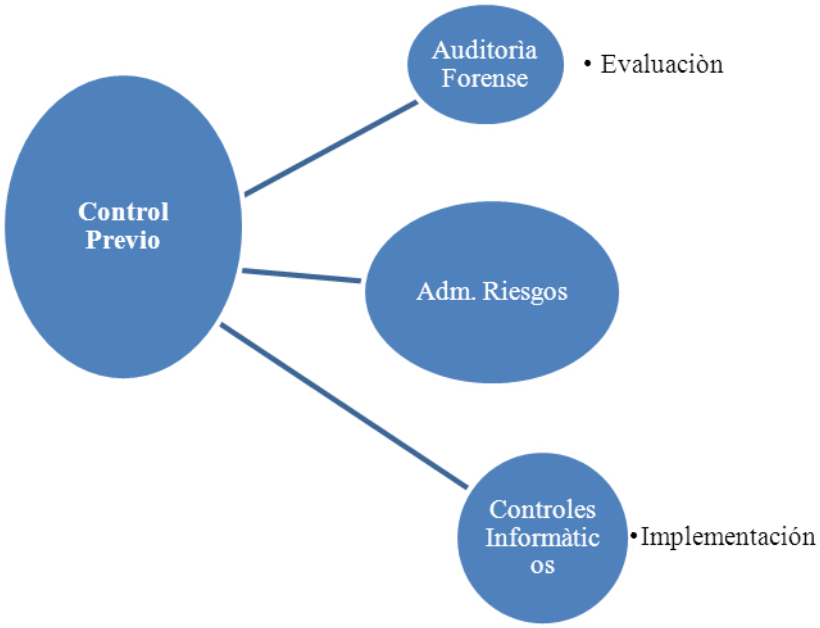


Gráfico 5: Variable dependiente



2.5. HIPOTESIS

La insuficiente Seguridad Corporativa es lo que limita la identificación en forma oportuna los riesgos en el Servicio de Rentas Internas Ambato

2.6. SEÑALAMIENTO DE VARIABLES DE LA HIPOTESIS

Variable Independiente

La insuficiente Seguridad Corporativa

Variable Dependiente

Identificación oportuna de Riesgos (Control previo de la Auditoría Forense)

Unidades de Observación

El Servicio de Rentas Internas Ambato

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ENFOQUE

El presente proyecto de investigación será predominantemente cualitativo, por cuanto la Seguridad Corporativa afecta a los individuos e Institución bajo lo cual se trata de solucionar los problemas con ayuda de los técnicos en la materia

Según información presentada por **Roberto Hernández y otros (2003: 4-6),** indica que el enfoque cualitativo, tiene su origen con Max Weber, quien reconoció que la medición y descripción de variables sociales deben considerar los significados subjetivos y el entendimiento del contexto donde ocurre un fenómeno. El enfoque cualitativo, por lo común, se utiliza primero para descubrir y refinar preguntas de investigación, para probar hipótesis; su propósito consiste en "reconstruir" la realidad, tal y como la observan los actores de un sistema social previamente definido. A menudo se llama "holístico" porque se precia de considerar el todo, sin reducirlo al estudio de sus partes Tomando como referencia a **Víctor Hugo Abril (2008: 5),** indica que la Investigación Cualitativa se ha concebido últimamente como aquel tipo de investigación en el cual participan los individuos y comunidad para solucionar sus propias necesidades y problemas, bajo la guía de técnicos al respecto, pero con la participación directa de todos los interesados en su desarrollo.

Por lo expuesto la presente investigación se fundamenta entonces en el paradigma positivista, el mismo que según lo define **Luis G. Meza C. (2010: Internet)**, el

Positivismo es una corriente de pensamiento cuyos inicios se suele atribuir a los planteamientos de Auguste Comte, y que no admite como válidos otros conocimientos sino los que proceden de las ciencias empíricas

La Investigación Cualitativa no sólo no provee de los medios para explorar situaciones complejas y caóticas de la vida real, sino que nos aportan múltiples opciones metodológicas sobre cómo acercarse a tal ámbito de acuerdo con el problema y los objetivos del estudio, además la recogida, análisis e interpretación de datos que no son objetivamente mensurables.

La investigación cualitativa en el presente proyecto pretende comprender las complejas relaciones entre todo lo que existe, además consiste en descripciones detalladas de situaciones, eventos, personas, interacciones y comportamientos que son observables. Incorpora lo que los participantes dicen, sus experiencias, actitudes, creencias, pensamientos y reflexiones tal como son expresadas por ellos mismos y no como uno los describe

3.2. MODALIDAD BASICA DE LA INVESTIGACION

3.2.1 Investigación de campo

El término ***investigar*** proviene del latín: ***"investí-gare"***, ***"investigatio"*** que hace referencia a: inquirir, indagar, averiguar, descubrir algo desconocido. En general investigar es: averiguar sobre algo no conocido, buscar la solución a un problema, descubrir la verdad, conforme lo señala **Víctor Hugo Abril (2008: 30)** en su trabajo sobre elaboración y evaluación de proyectos de investigación

Según lo que indica, **Mario Tamayo (2008: Internet)**, en su libro sobre el Proceso de la Investigación, define a la Investigación de campo como el tipo de investigación que se apoya en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones. Como es compatible

desarrollar este tipo de investigación junto a la investigación de carácter documental, se recomienda que primero se consulten las fuentes de la de carácter documental, a fin de evitar una duplicidad de trabajos.

A través de la investigación de Campo lograremos estar en contacto con la realidad a investigarse, esta modalidad de investigación nos permite recolectar y analizar información de todos los hechos y acontecimientos que se producen en la Institución respecto de la Seguridad Corporativa, utilizando técnicas de investigación adecuadas tales como, la observación, encuesta y entrevista principalmente

3.2.2 Investigación Bibliográfica documental

Para **Leopoldo Fuente (2008: Internet)**, la investigación documental es la que se realiza, como su nombre lo indica, apoyándose en fuentes de carácter documental, esto es, en documentos de cualquier especie. Como subtipos de esta investigación encontramos la investigación bibliográfica, la hemerográfica y la archivística; la primera se basa en la consulta de libros, la segunda en artículos o ensayos de revistas y periódicos, y la tercera en documentos que se encuentran en los archivos, como cartas, oficios, circulares, expedientes y otros.

Se aplicará este tipo de investigación, porque a través de ella, se toma como soporte todos aquellos documentos relacionados al tema de investigación, en este caso nos referimos principalmente a la base legal referenciada, las disposiciones escritas respecto de normas de seguridad para funcionarios, y todos los medios escritos para el desarrollo del presente proyecto que servirán de base para la investigación como son libros, periódicos, revistas, folletos y otros

3.3 NIVEL O TIPO DE INVESTIGACION

3.3.1 Investigación exploratoria

Según lo señala **Roberto Hernández y otros (2003: 115-117)**, los estudios exploratorios sirven para preparar el terreno y por lo común anteceden a los otros tipos de investigación. Se efectúan normalmente cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tiene dudas o no se han abordado antes. Los estudios exploratorios sirven para obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular, establecer prioridades para investigaciones futuras, o sugerir afirmaciones y postulados.

Se considera conveniente aplicar la investigación exploratoria, porque a más de referirse a un primer nivel de conocimiento, nos permite ubicarnos en contacto con la realidad que se va a investigar, es la manera más adecuada de explorar todos los aspectos relacionados con la Seguridad Corporativa y sus principales inconvenientes, lo que nos ayudará a obtener elementos de juicio para reafirmar el problema planteado, reforzar el conocimiento respecto a las posibles causas y sobretodo brindar una mayor seguridad al momento de plantear los resultados de la investigación.

3.3.2 Investigación descriptiva

Tomando como referencia a **César Bernal (2000: 111)**, define a la investigación descriptiva como aquella en la que se reseñan las características o rasgos de la situación o fenómeno de estudio.

Para **Hugo Cerda (1997: 71)**, tradicionalmente ha definido la palabra “describir” como el acto de representar, reproducir o figurar a personas, animales o cosas,

describiendo aquellos aspectos más característicos distintivos y particulares de estas personas, situaciones o cosas. La función principal de este tipo de investigación es la capacidad de seleccionar las características fundamentales del objeto de estudio

Según lo señala **Roberto Hernández y otros (2003: 117-118)**, los estudios exploratorios buscan especificar las propiedades, características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis.

Para alcanzar un segundo nivel de conocimiento, se empleará la Investigación Descriptiva, a través de la cual describiremos todos los hechos y características más sobresalientes que se produzcan en relación al problema de investigación, con lo cual, estaremos en capacidad de conocer cual es la principal causa que origina los insuficientes controles informáticos, que pueden crear riesgos y además se establecerá su nivel de incidencia en el control previo de Auditoría Forense, logrando con ello un mayor nivel de conocimiento e información para la investigación

3.3.3 Investigación asociación de variables (correlacional)

Para **César Bernal (2000: 1121)**, la investigación correlacional tiene como propósito mostrar o examinar la relación entre variables o resultados de variables.

Según señala **Roberto Hernández y otros (2003: 121)**, los estudios correlacionales pretenden responder a preguntas de investigación, evalúa la relación que existe entre dos o más conceptos, categorías o variables.

Con la aplicación de la Investigación Correlacional, podremos medir el grado de relación existente entre las variables planteadas, es decir por qué la variación de comportamiento de una variable depende de la variación del comportamiento de la otra, se analizará el porqué de esta reacción, en este sentido podremos comprobar y determinar las asociaciones y relaciones entre dos o más fenómenos que involucran el problema de la investigación.

3.4 POBLACION Y MUESTRA

3.4.1 Definir la población

Es importante conocer la definición de población, de acuerdo con lo indicado por **Germán Fracica (1988: 36)**, la población es el conjunto de todos los elementos a los cuales se refiere la investigación. Se puede también definir como el conjunto de todas las unidades de muestreo

Para el presente proyecto de investigación se ha definido a la población como el personal que conforma el Servicio de Rentas Internas de Ambato, en el que actualmente laboran ciento dieciocho personas, en las diferentes áreas y/o departamentos según la estructura orgánica funcional utilizada, por cuanto están involucradas directamente con el problema planteado. Se encuentra distribuido según se muestra a continuación:

Tabla 1: Número de personal por departamento SRI Ambato

No.	DEPARTAMENTO	NUMERO DE FUNCIONARIOS
1	Dirección Regional	3
2	Servicios Tributarios	26
3	Secretaría Regional	15
4	Gestión Tributaria	28
5	Reclamos	10
6	Jurídico	6
7	Auditoría	14
8	Planificación	1
9	Cobranzas	5
10	Administrativo Financiero	10
	TOTAL	**118**

Fuente: RRHH-SRI 2010

Elaborado por: Mercy Solis

3.4.2 Determinar la muestra

De acuerdo a lo que establece **Lamberto Vera (2010: Internet)** la muestra es un subconjunto fielmente representativo de la población. Hay diferentes tipos de muestreo. El tipo de muestra que se seleccione dependerá de la calidad y cuán representativo se quiera sea el estudio de la población.

El muestreo es indispensable para el investigador ya que es imposible entrevistar a todos los miembros de una población debido a problemas de tiempo, recursos y esfuerzo.

Según la señalado por **Tevni Grajales G. (2010: Internet)**, el muestreo es tomar una porción de una población como subconjunto representativo de dicha población.

Para el desarrollo de la presente investigación es necesario que se determine muestreo, para lo cual se aplicará el método estratificado, que permitirá obtener una muestra de las personas que laboran en los diferentes departamentos en los que se ha dividido a la población.

Muestreo estratificado.- De acuerdo a lo que establece **Luis Herrera y otros (2004- 110)** el muestreo estratificado consiste en dividir al universo en estratos, zonas o grupos más o menos homogéneos, para luego tomar la muestra de cada estrato utilizando alguna técnica analizada anteriormente. Los elementos de cada estrato deben estar en proporción directa al universo de la población en general y de cada grupo o estrato.

Muestreo estratificado.- Conforme a lo publicado en la página web de la enciclopedia **WIKIPEDIA (2010: Internet)** el muestreo estratificado consiste en la división previa de la población de estudio en grupos o clases que se suponen homogéneos con respecto a alguna característica de las que se van a estudiar. A cada uno de estos estratos se le asignaría una cuota que determinaría el número de miembros del mismo que compondrán la muestra. Dentro de cada estrato se suele usar la técnica de muestreo sistemático, una de las técnicas de selección más usadas en la práctica.

Según la cantidad de elementos de la muestra que se han de elegir de cada uno de los estratos, existen dos técnicas de muestreo estratificado:

- **Asignación proporcional:** el tamaño de la muestra dentro de cada estrato es proporcional al tamaño del estrato dentro de la población.

- **Asignación óptima:** la muestra recogerá más individuos de aquellos estratos que tengan más variabilidad. Para ello es necesario un conocimiento previo de la población

Para la obtención de la muestra relacionada con la población de las personas que laboran en los diferentes departamentos del SRI Ambato, se aplicará la fórmula presentada en el trabajo denominado: "Elaboración de proyectos" de **Víctor Hugo Abril (2010: Internet)**:

$$n = \frac{N}{E^2 (N - 1) + 1}$$

Simbología

n= Tamaño de la muestra
N= Población 118
E= Error de muestreo 5%

Aplicación de la fórmula

$$n = \frac{118}{0{,}05^2 (118-1) + 1}$$

$$n = \frac{118}{1.2925}$$

n= **91**

En este caso se ha obtenido una muestra de 91 personas del total de la población, por lo que a continuación se establece el porcentaje que cada uno de los departamentos en los que se estratificó la población, representa frente a esta:

Tabla 2: Número de personas por departamento SRI Ambato (muestreo estratificado)

Población	**118**	**100%**
Dirección Regional	3	2.54%
Servicios Tributarios	26	22.03%
Secretaría Regional	15	12.71%
Gestión Tributaria	28	23.73%
Reclamos	10	8.47%
Jurídico	6	5.08%
Auditoría	14	11.86%
Planificación	1	0.86%
Cobranzas	5	4.25%
Administrativo Financiero	10	8.47%

3.5 OPERACIONALIZACION

La Operacionalización de las variables según, **Roberto Hernández y otros (2003: 171)**, constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar para recibir las impresiones sensoriales, las cuales indican la existencia de un concepto teórico en mayor o menor grado, es decir especifica qué actividades u operaciones deben realizarse para recolectar datos o información.

Según **Héctor Ávila (2009: Internet)**, operacionalizar es definir las variables para que sean medibles y manejables Un investigador necesita traducir los conceptos (variables) a hechos observables para lograr su medición. Las definiciones señalan las operaciones que se tienen que realizar para medir la variable, de forma tal, que sean susceptibles de observación y cuantificación. La definición operacional de un concepto consiste en definir las operaciones que permiten medir ese concepto o los indicadores observables por medio de los cuales se manifiesta ese concepto.

En resumen, una definición operacional puede señalar el instrumento por medio del cual se hará la medición de las variables. La definición operativa significa ¿como le voy a hacer en calidad de investigador para operacionalizar mi pregunta de investigación?

A continuación se muestra la Operacionalización de las variables para el presente proyecto de investigación:

3.5.1. Operacionalización

Tabla 3: Variable independiente Insuficiente Seguridad Corporativa

CONCEPTUALIZACION	CATEGORIAS	INDICADORES	ITEMS	TECNICA
La deficiente Seguridad Corporativa	Evaluación del sistema de seguridad existente	% de conocimiento y aplicación del personal	Los empleados conocen y aplican las políticas de seguridad establecidas?	Encuesta: Personal Operativo Cuestionario (Anexo 2)
			Se han realizado informes de evaluación de cumplimiento?	Entrevista: Director Regional y Jefes Dpto. Cuestionario (Anexo 3)
		número de infracciones cometidas	Se han tomado acciones previas de control frente a riesgos eventuales?	
			Se han aplicado sanciones por incumplimiento?	
	Diseño de un Sistema de Integral de Seguridad Corporativa	% de control sobre bienes y sistemas	Se han inventariado los bienes tangibles y no tangibles sujetos a control?	Entrevista: Director Regional y Jefes Dpto. Cuestionario (Anexo 3)
			Se han desarrollado flujos de los procesos de control?	
		% de cumplimiento del Plan de Seguridad	Se ha socializado el Plan de Seguridad?	
			Se han establecido responsables de su evaluación y cumplimiento?	

Tabla 4: Variable dependiente Control previo de la Auditoria Forense

CONCEPTUALIZACION	CATEGORIAS	INDICADORES	ITEMS	TECNICA
Control Previo de la Auditoría Forense	Incidencia de la Seguridad Corporativa en la Auditoría Forense	% de controles implementados	Se identifica a la Seguridad Corporativa como un control previo?	Encuesta: Personal Operativo Cuestionario (Anexo 2)
			Se cuenta con alertas tempranas para detección oportuna de riesgos?	Entrevista: Director Regional y Jefes Dpto. Cuestionario (Anexo 3)
		% de relación de controles con delitos identificados	Los delitos cometidos se identificaron con algún control?	
			Se consideran adecuados y eficientes los controles establecidos?	Encuesta: Personal Operativo Cuestionario (Anexo 2)
	Evaluación de Resultados Finales	% de fraudes corporativos	Se evidencia una reducción de fraudes corporativos con la implementación de Seguridad Corporativa?	Entrevista: Director Regional y Jefes Dpto. Cuestionario (Anexo 3)
			Se ha realizado evaluaciones de la incidencia de la Seguridad Corporativa vs. Número de fraudes cometidos?	
		número de delitos cometidos	Se evidencia una mejor cultura de seguridad en el personal?	
			Se ha establecido el clima en la cima?	

3.6. RECOLECCIÓN DE INFORMACIÓN

Metodológicamente para **Luis Herrera E. y otros (2002: 174-178 y 183-185)**, la construcción de la información se opera en dos fases: plan para la recolección de información y plan para el procesamiento de información.

3.6.1. Plan para la recolección de información

Fuentes primarias

- Constitución Política de la República del Ecuador
- Ley Orgánica de la Contraloría General del Estado
- Ley de Creación del Servicio de Rentas Internas
- Código de Ética
- Leyes y Resoluciones acerca del tema emitidas por la Administración Tributaria.
- Artículos Publicados en Internet

Fuentes Secundarias

- Encuesta
- Entrevistas

3.7. PROCESAMIENTO Y ANALISIS

3.7.1. Plan de Procesamiento de información

El procesamiento de la información constituye un factor fundamental en la elaboración de el presente trabajo, por esta razón se procedió a revisar y analizar la información obtenida, para poder detectar errores o información no necesaria para organizarla de la manera más clara posible para facilitar la obtención de resultados.

Es por esta razón que los datos recogidos se transforman siguiendo ciertos procedimientos:

- Revisión crítica de la información recogida, es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente, etc., que puede confundir los resultados al momento del análisis.
- Estudio estadístico de datos para presentación de resultados.

La presentación de datos fue utilizando estos procedimientos:

Representación escrita

Se utilizó cuando los datos no fueron numerosos.

Representación tabular

Se utilizó cuando los datos numéricos fueron ordenados en filas y columnas, con las especificaciones correspondientes, según el tipo y características de dichos datos.

Representación Gráfica

Se utilizó para presentar la información de una forma comparativa, sencilla y entendible para el lector.

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis de los resultados

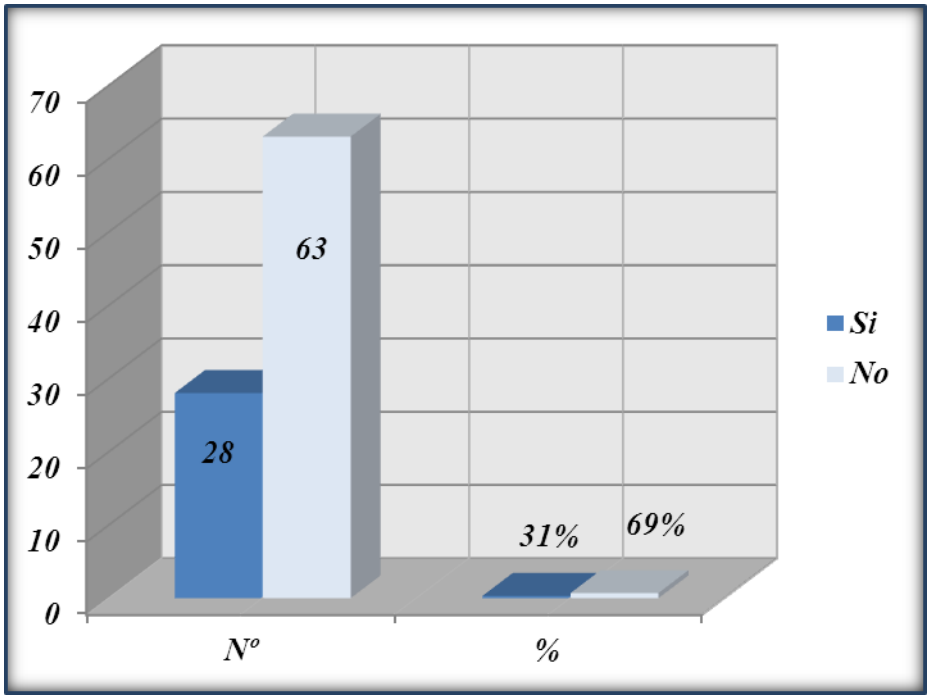
Análisis de la encuesta

1. ¿Conoce usted los controles implementados para la seguridad física de las instalaciones?

Tabla 5: Controles para la seguridad física

Variables	Nº	%
Si	28	31%
No	63	69%
Total	91	100%

Gráfico 6: Pregunta 1



Análisis

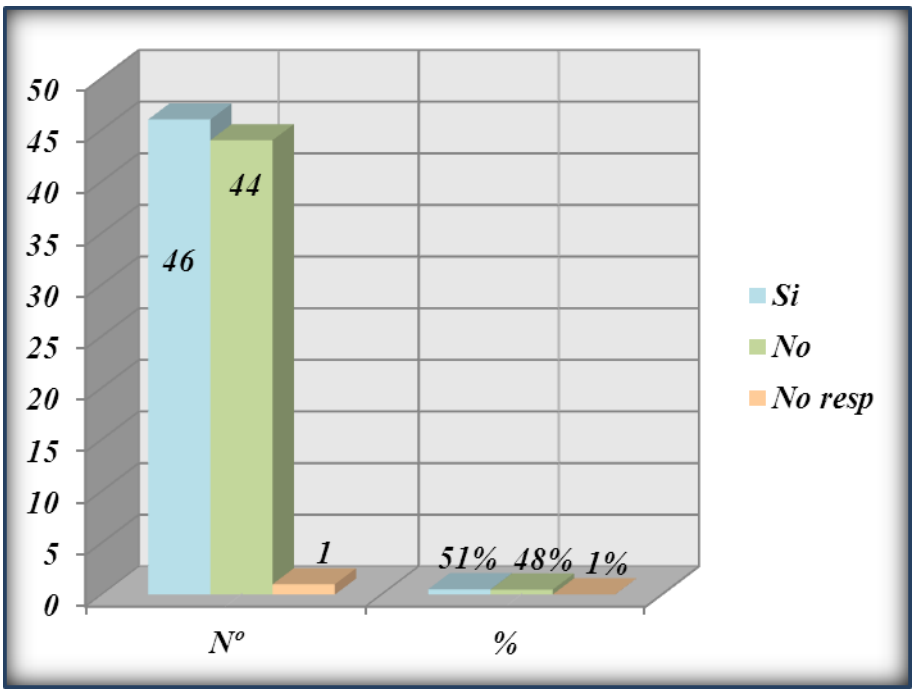
En la primera pregunta que trata sobre los controles implementados para la seguridad física de las instalaciones, el 31% contesta que Si conoce, el 69% de los encuestados No, los resultados ayudan establecer que existe un claro desconocimiento sobre temas de seguridad.

2. **¿Ha sido instruido sobre las seguridades tecnológicas para el manejo de equipos de computación a su cargo?**

Tabla 6: Instrucción sobre seguridad tecnológica

Variables	Nº	%
Si	46	51%
No	44	48%
No responde	1	1%
Total	91	100%

Gráfico 7: Pregunta 2



Análisis

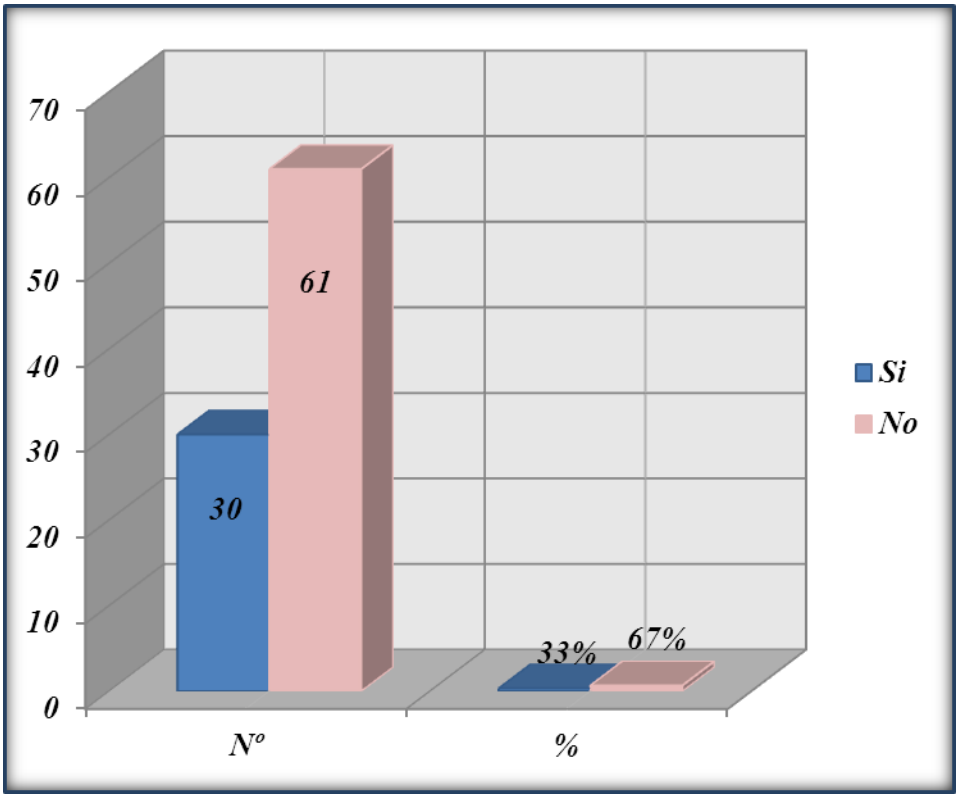
En la segunda pregunta de la encuesta, el 51% respondió Si, el 48% de los encuestados por el No, No responde el 1%, solo un 51% ha sido capacitado sobre seguridad informativa para un manejo óptimo de equipos de computación que están a su cargo en puesta de trabajo.

3. **Identificando a la Seguridad Personal como las medidas que permiten minimizar riesgos o vulnerabilidades sobre su integridad física: ¿Considera usted que existen adecuadas seguridades personales en su lugar de trabajo?**

Tabla 7: Seguridad personal en el lugar de trabajo

Variables	Nº	%
Si	30	33%
No	61	67%
Total	91	100%

Gráfico 8: Pregunta 3



Análisis

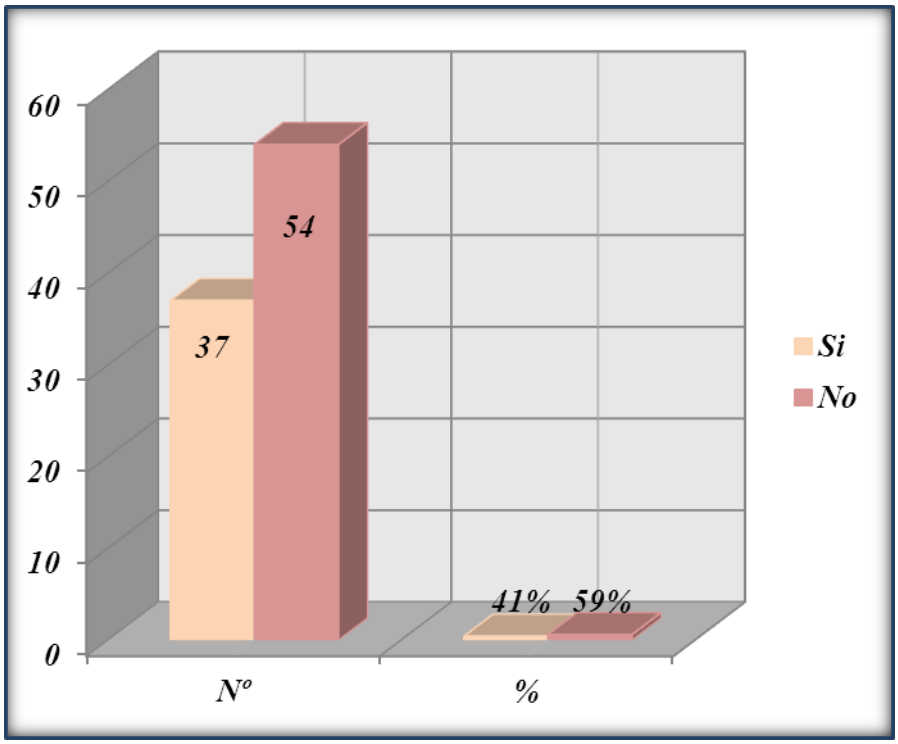
En la tercera pregunta, sobre las adecuadas seguridades personales en un lugar de trabajo, de los encuestados el 33% contesta que Si, el 67% considera que No; se considera que la seguridad no es la más óptima para quienes ejercen su trabajo en el SRI.

4. **¿En caso de ausencia temporal de su lugar de trabajo, conoce las seguridades que debe aplicar?**

Tabla 8: Caso de ausencia temporal en el trabajo

Variables	Nº	%
Si	37	41%
No	54	59%
Total	91	100%

Gráfico 9: Pregunta 4



Análisis

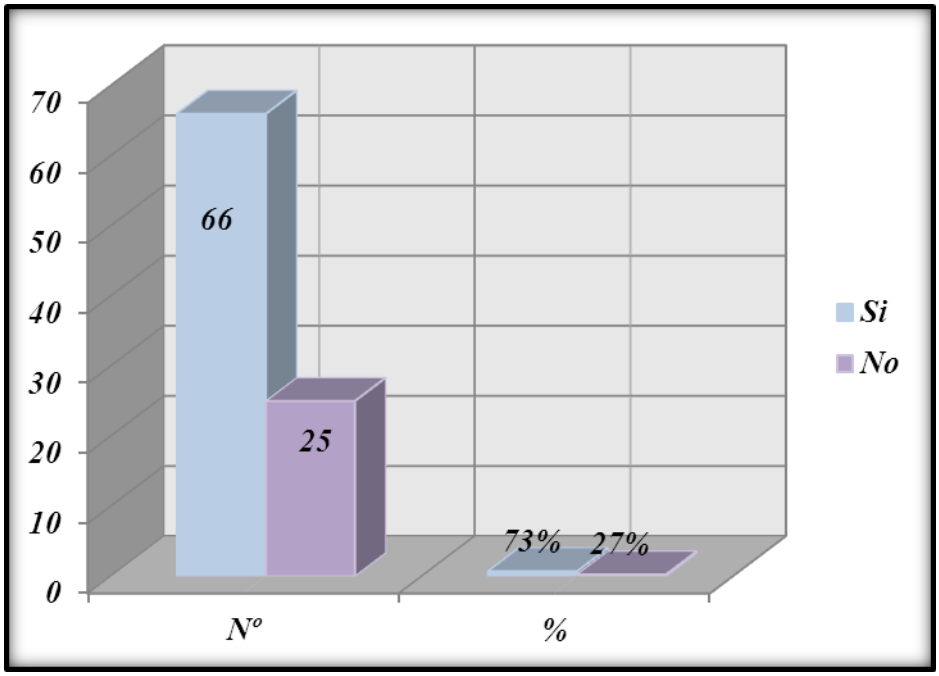
En la cuarta pregunta, en el caso de ausencia temporal en el lugar de trabajo, de los encuestados el 41% contesto Si, el 59% No, el porcentaje determina que hay poco conocimiento sobre seguridad, tema preocupante pues al tener estrategias en lo que se refiere ausencia temporal, se podrá tomar las medidas para resolver este tema.

5. ¿Identifica claramente las áreas de acceso restringidos al público?

Tabla 9: Áreas de acceso restringido

Variables	Nº	%
Si	66	73%
No	25	27%
Total	91	100%

Gráfico 10: Pregunta 5



Análisis

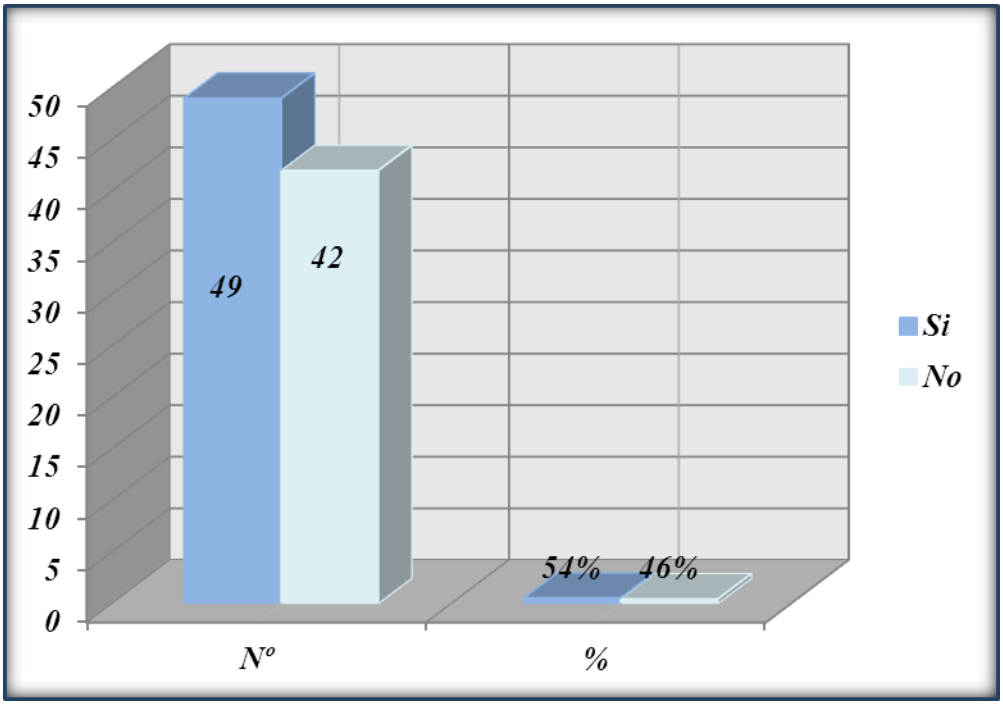
En el caso de la quinta pregunta sobre la identificación clara de las áreas de acceso restringidos al público, el 73% contesto Si, en cambio el 27% No, los encuestados identifican las zonas restringidas, solo un porcentaje minoritario no lo hace.

6. **¿Considera usted adecuadas las seguridades para salvaguarda de la información que maneja?**

Tabla 10: Seguridad para salvaguardar la información

Variables	Nº	%
Si	49	54%
No	42	46%
Total	91	100%

Gráfico 11: Pregunta 6



Análisis

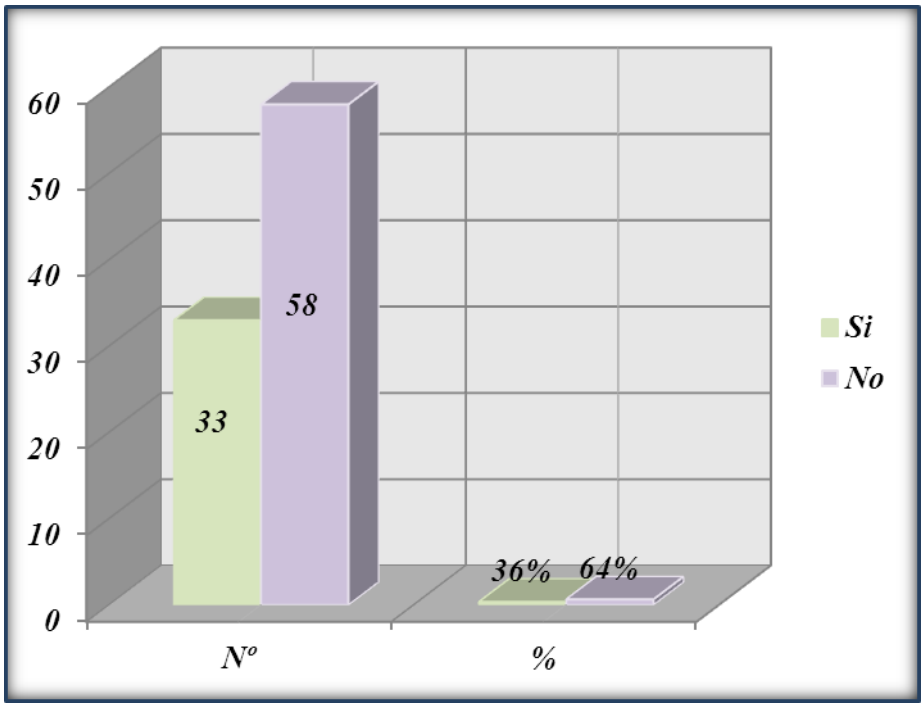
En la sexta pregunta, sobre las seguridades para salvaguardar la información que se maneja, el 54% respondió que Si son adecuadas, el 46% de los encuestados No, es necesario implementar acciones claras para brindar seguridad informática.

7. ¿En alguna ocasión ha perdido información física o magnética importante en el desarrollo de su trabajo?

Tabla 11: Perdida de información física o magnética

Variables	Nº	%
Si	33	36%
No	58	64%
Total	91	100%

Gráfico 12: Pregunta 7



Análisis

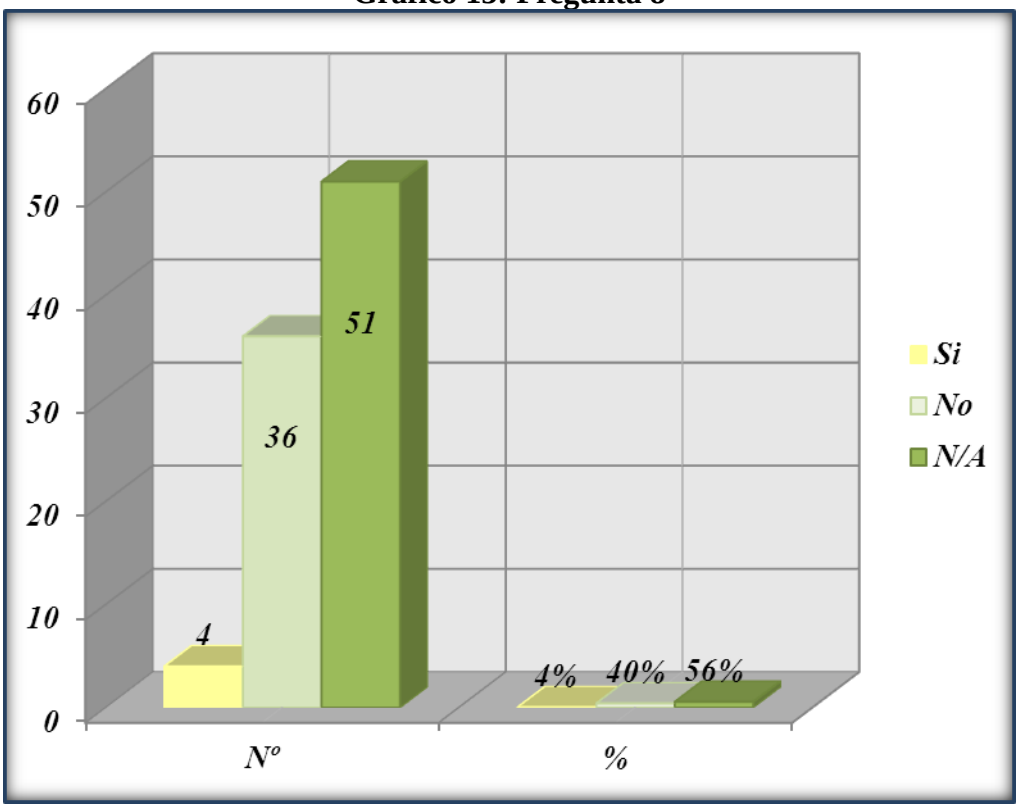
En la séptima pregunta, sobre la perdida de información física o magnética importante en el desarrollo del trabajo, de los encuestados el 36% manifiesta que Si que alguna ocasión, el 64% contestó No, se han presentado casos pero es necesario evaluar las causas para que se de este problema.

8. En caso de ser afirmativa la respuesta anterior: ¿Conocía el procedimiento a seguir para la recuperación de esta información?

Tabla 12: Recuperación de información

Variables	Nº	%
Si	4	4%
No	36	40%
N/A	51	56%
Total	91	100%

Gráfico 13: Pregunta 8



Análisis

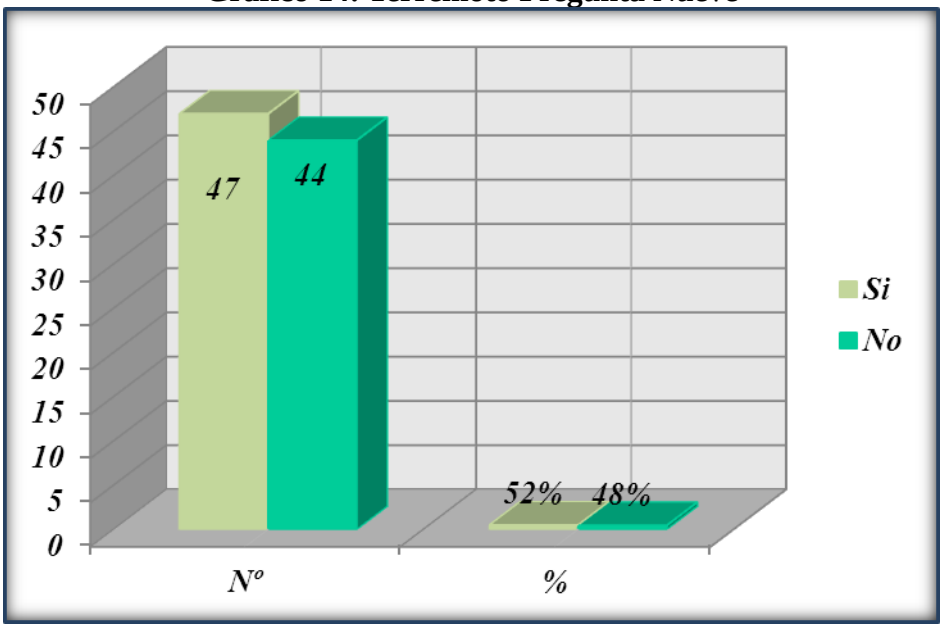
En la octava pregunta, los encuestados responden sobre el procedimiento a seguir para la recuperación de la información, 4% manifiesta que Si conocen, el 40% contesto No, la necesidad de crear medidas para recuperación de la información, deben de nacer de cada departamento de la institución.

9. ¿En caso de siniestros, que se detallan a continuación, conoce el procedimiento a seguir?

Tabla 13: Terremoto

Variables	Nº	%
Si	47	52%
No	44	48%
Total	91	100%

Gráfico 14: Terremoto Pregunta Nueve



Análisis

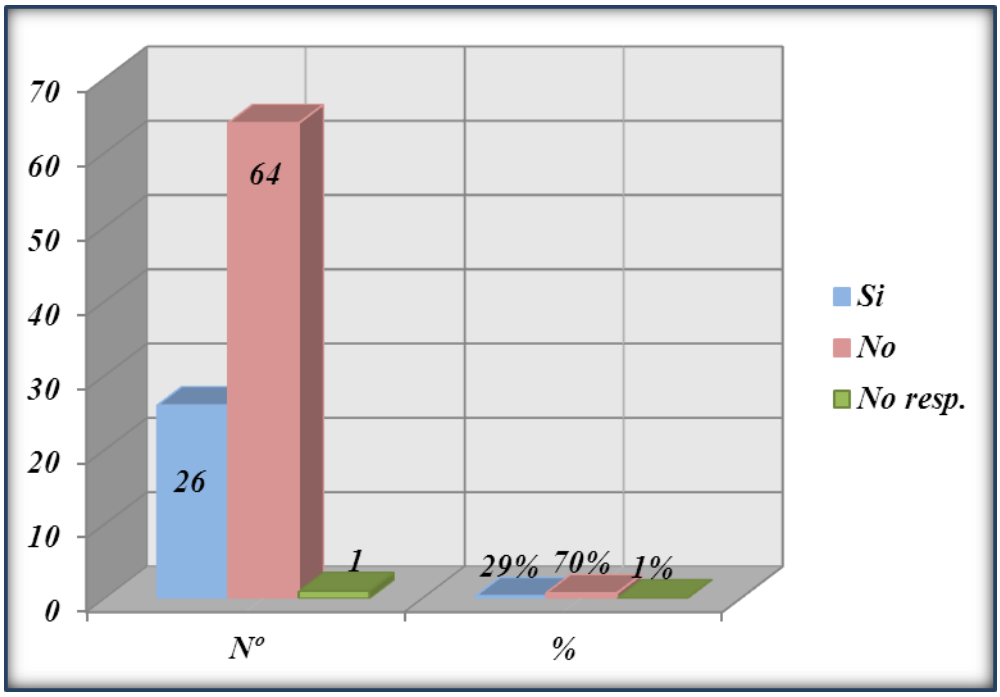
En la novena pregunta, sobre siniestros, en el caso de Terremoto, el 52% manifiesta que Si conoce el procedimiento a seguir, el 48% de los encuestados contestaron No, hay conocimiento sobre qué hacer si se presenta un terremoto, pero el otro porcentaje necesitan capacitarse sobre el tema.

Incendio

Tabla 14. Incendio

Variables	Nº	%
Si	26	29%
No	64	70%
No responde	1	1%
Total	91	100%

Gráfico 15: Incendio Pregunta Nueve



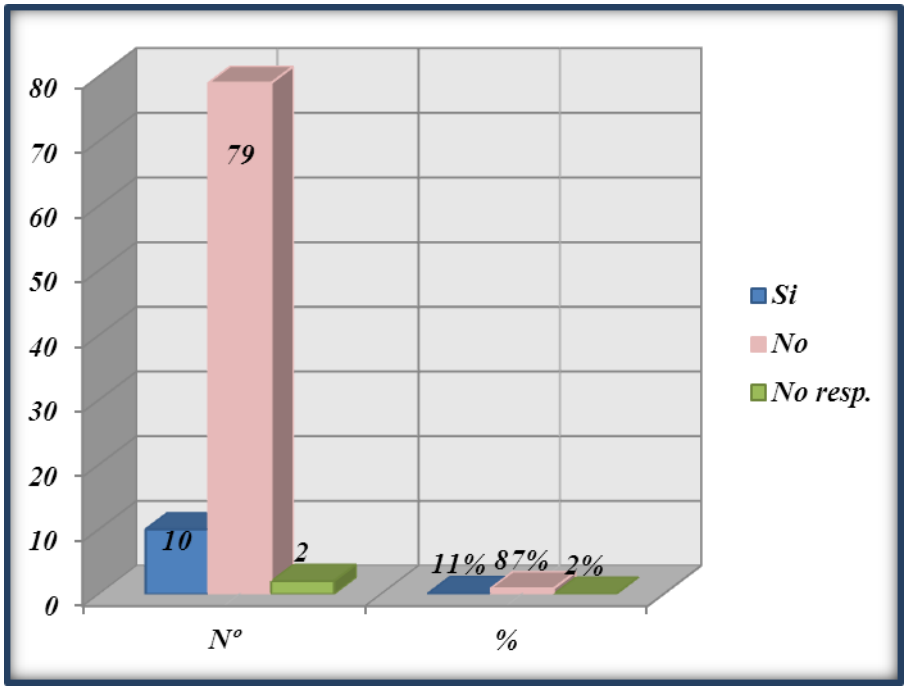
Análisis

Se encuestó sobre los procedimientos en el caso de incendios solo el 29% respondió que Si, el 70% optó por el No, solo 1% No responde a la pregunta, no se conoce sobre las medidas de prevención a tomarse en el caso de incendios.

Tabla 15: Inundación

Variables	Nº	%
Si	10	11%
No	79	87%
No responde	2	2%
Total	91	100%

Gráfico 16: Inundación Pregunta Nueve



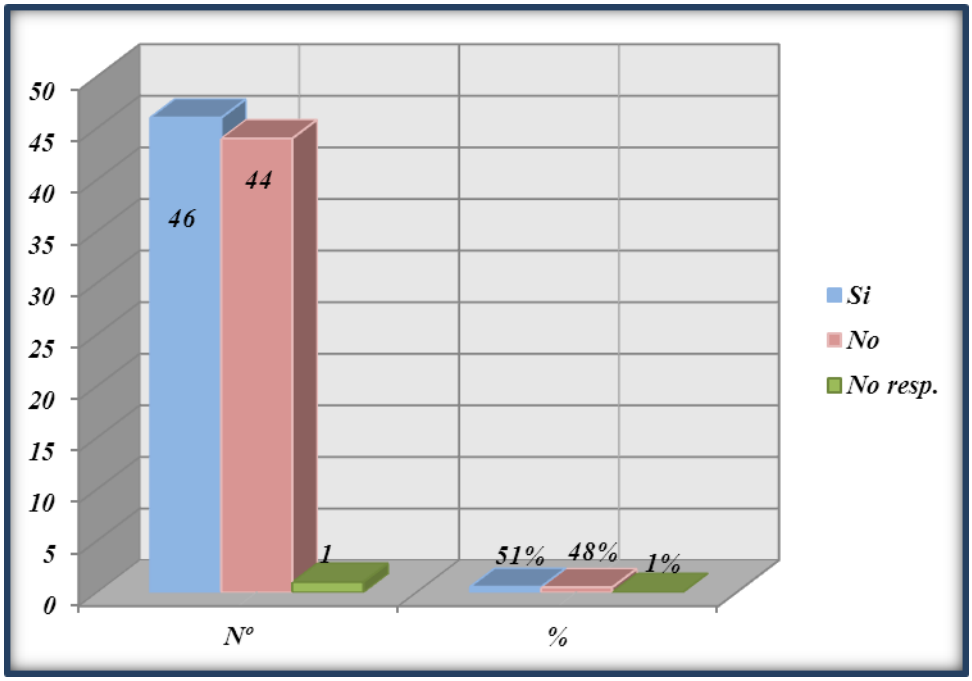
Análisis

Otro siniestro analizado fue inundación de los encuestados el 11% responde Si, por el No el 87%, el 2% decide No responde, no se conoce y no habido capacitación sobre los procedimientos a seguir en el caso de inundación.

Tabla 16: Erupción Volcánica

Variables	Nº	%
Si	46	51%
No	44	48%
No responde	1	1%
Total	91	100%

Gráfico 17: Erupción Volcánica, Pregunta Nueve



Análisis.

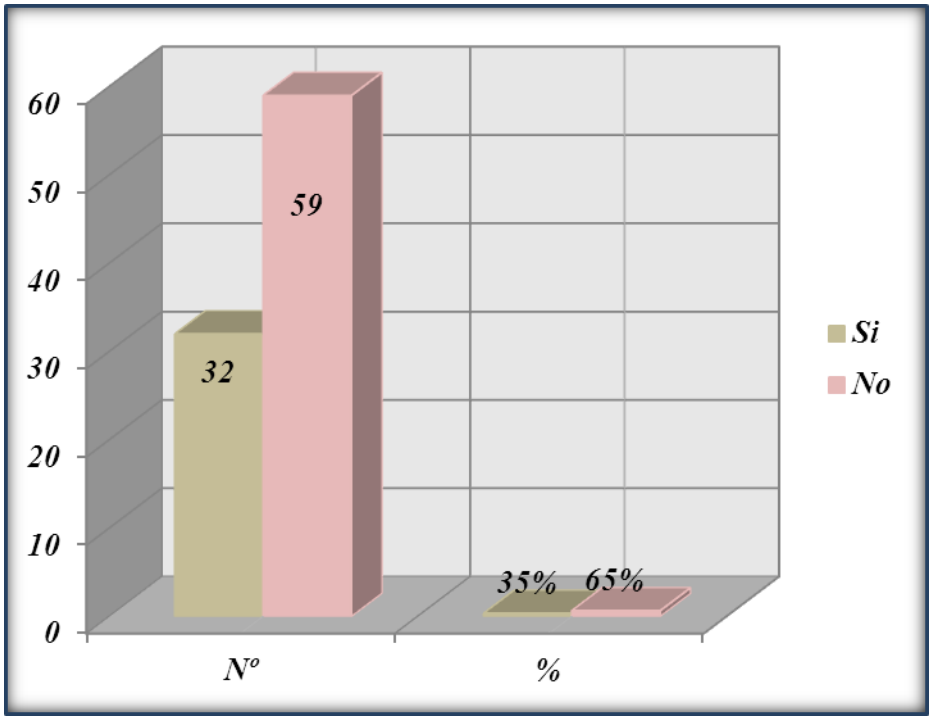
En el caso de erupción volcánica, el 51% de los encuestados respondió que Si conoce sobre los procedimientos a seguir, un 48% dijo que no sabia, el 1% No responde, se ha dado más énfasis en sensibilizar en las acciones a seguir en el caso de una erupción.

10. ¿Conoce los procedimientos a seguir para crear respaldos periódicos de la información que está bajo su responsabilidad?

Tabla 17: Respaldos periódicos de información

Variables	Nº	%
Si	32	35%
No	59	65%
Total	91	100%

Gráfico 18: Pregunta Diez



Análisis

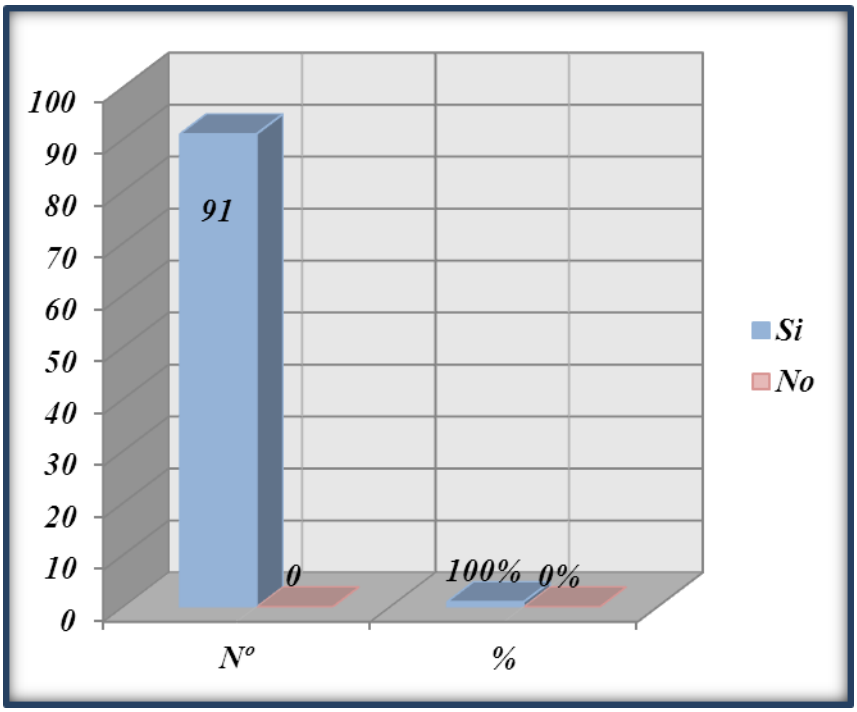
En la décima pregunta, sobre los procedimientos a seguir para crear respaldos periódicos de la información que está bajo responsabilidad, el 35% manifiesta que Si conoce los mismos, el 65% responde No, como se concluyó en preguntas anteriores no existe claro conocimiento sobre las medidas para garantizar el respaldo de la información.

11. ¿Considera usted necesario un adecuado programa de Seguridad Corporativa, que defina controles previos para minimizar los riesgos a los que estamos expuestos?

Tabla 18: Programa de Seguridad Corporativa

Variables	Nº	%
Si	91	100%
No	0	0%
Total	91	100%

Gráfico 19: Pregunta 11



Análisis

En la décima primera pregunta, que trata sobre si es necesario un adecuado programa de Seguridad Corporativa, todos los encuestados contestaron el 100% que Si, en este caso el programa se implementará a través de un Sistema de Seguridad Corporativa.

Análisis de los Resultados de la Entrevista

Para el desarrollo de la entrevista se utilizó preguntas abiertas, en algunos se obtuvieron respuestas cerradas las cuales fueron tabuladas para su buen entendimiento y análisis del problema de investigación**.**

Preguntas y respuestas tabuladas.

1. **¿Conoce usted si en el Servicio de Rentas Internas de Ambato se ha realizado un inventario de los riesgos a que están sujetos los bienes tangibles e intangibles?**

Tabla 19: Inventario de riesgos

Variables	Nº	%
Si	3	33%
No	6	67%
Total	9	100%

Gráfico 20: Inventario de riesgos

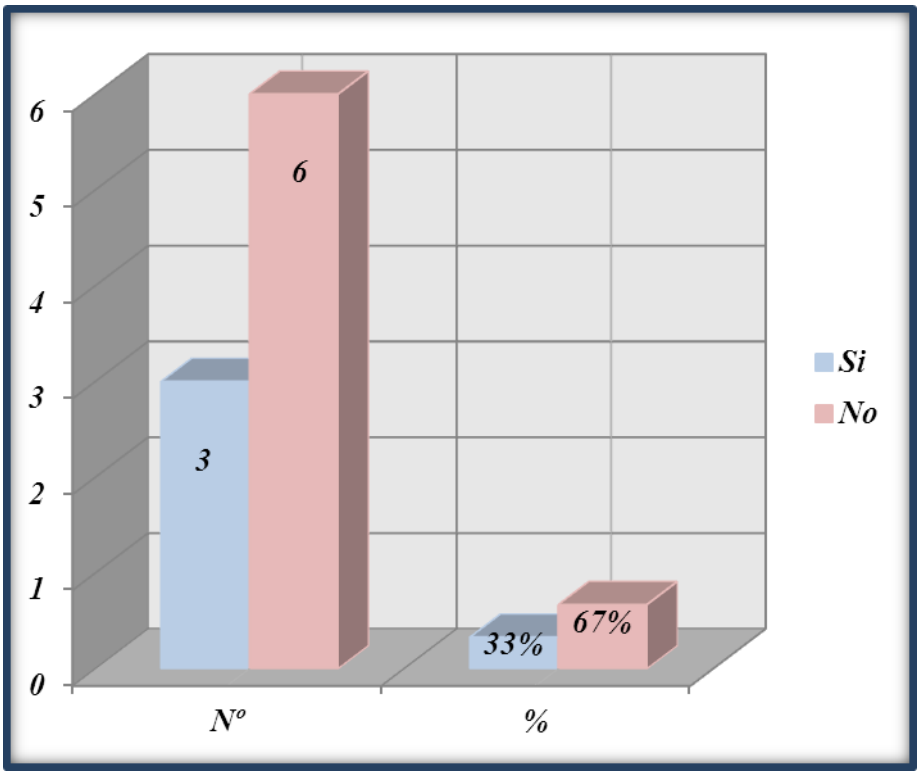


Tabla 20: Guía de entrevista pregunta 1

Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Existe un plan de seguridad de bienes y personas realizado hace dos años no se ha actualizado sobre riesgos físicos
Eco. Mateo Villacís **Jefe Departamental** **Planificación**	Sobre intangibles

2. **¿En su departamento se han elaborado flujogramas de los procesos de control?**

Tabla 21: Flujogramas de procesos de control

Variables	Nº	%
Si	1	11%
No	8	89%
Total	9	100%

Gráfico 21: Flujogramas de procesos de control

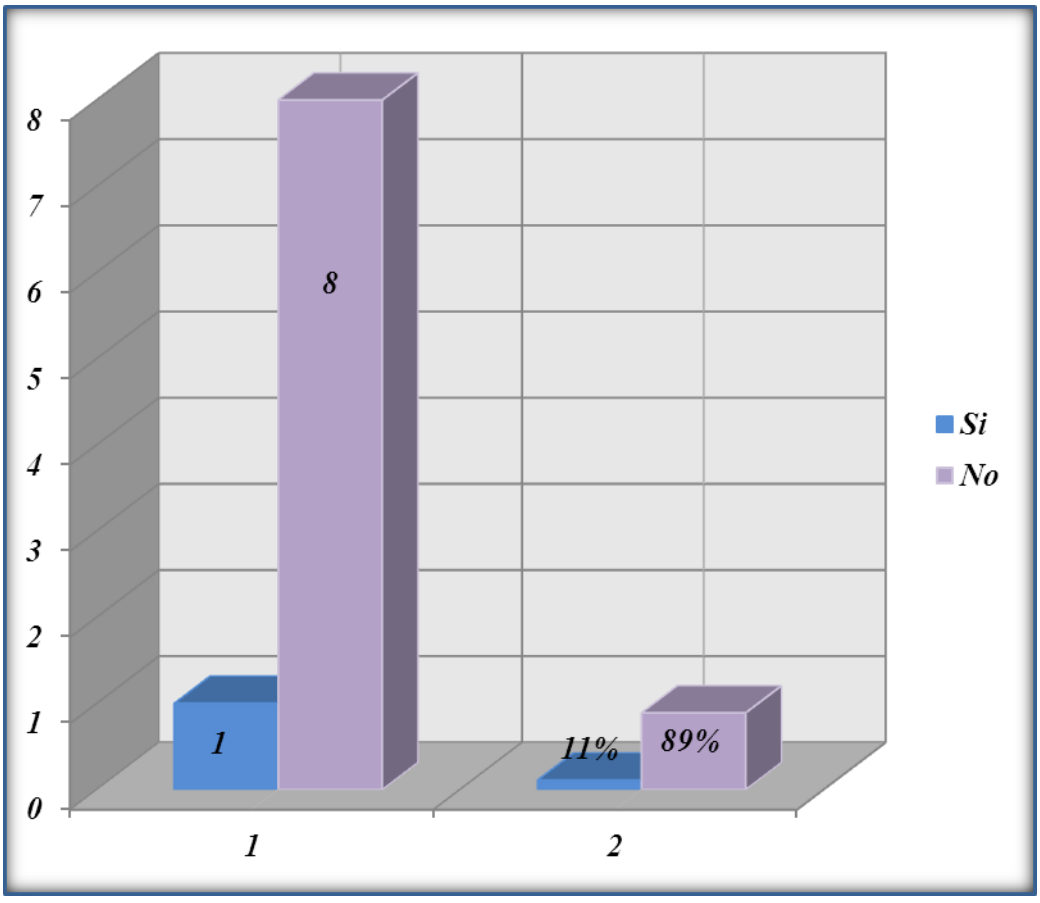


Tabla 22: Guía de entrevista pregunta 2

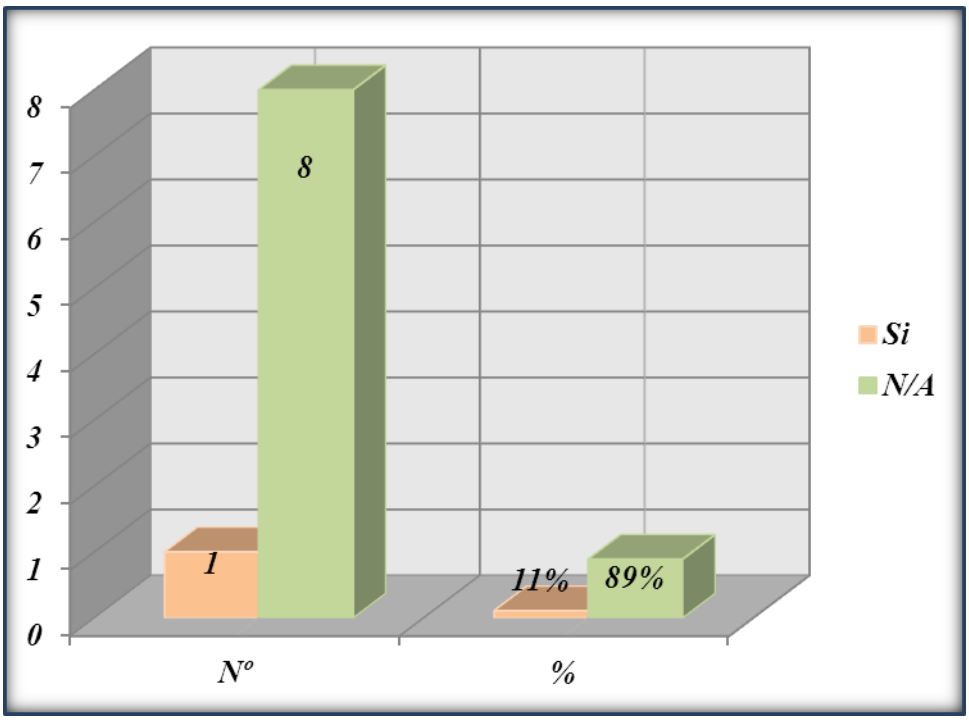
Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Se basan en los manuales de procedimientos existentes
Ing. Ana Fernanda Ortega **Jefe Departamental** **Reclamos**	Identificando la información de riesgo, no existen seguridades mínimas.
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Como flujograma no pero se han definido en base a proyectos.

3. **En caso de ser afirmativa la respuesta anterior ¿Se han designado los responsables en cada uno de los procesos de control definidos?**

Tabla 23: Responsables en cada uno de los procesos de control definidos

Variables	Nº	%
Si	1	11%
N/A	8	89%
Total	9	100%

Gráfico 22: Responsables en cada uno de los procesos de control definidos



4. **¿Se ha definido un Plan de Socialización al personal a su cargo sobre la Seguridad Corporativa que aplica la entidad?**

Tabla 24: Plan de Socialización sobre la Seguridad Corporativa

Variables	Nº	%
Si	0	0%
No	9	100%
Total	9	100%

Gráfico 23: Plan de Socialización sobre la Seguridad Corporativa

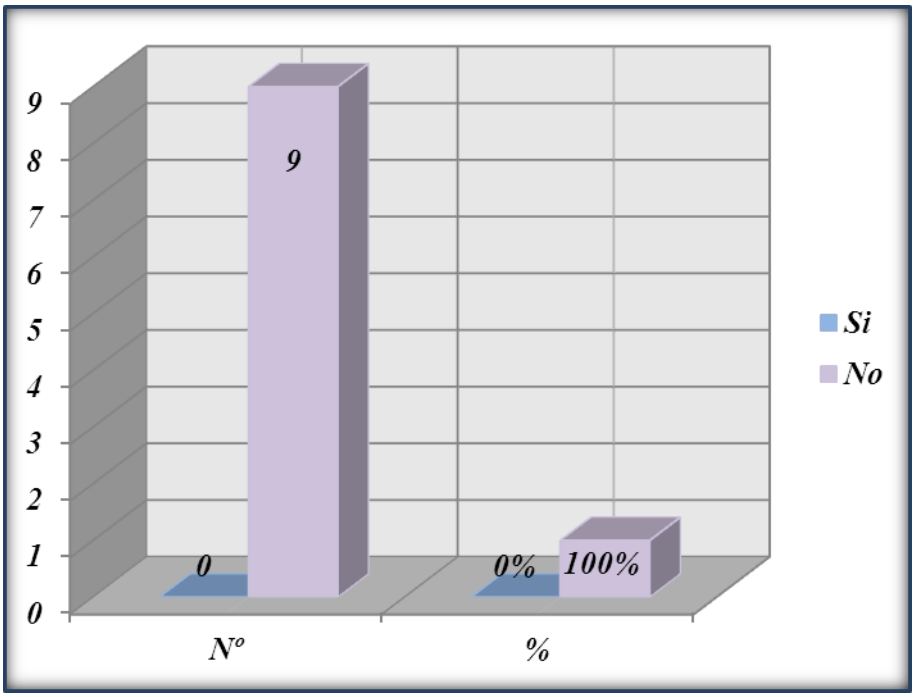


Tabla 25: Guía de entrevista pregunta 4

Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Correos recibidos desde la Dirección Nacional sobre Políticas Aplicadas
Dr. Fabián Mera **Jefe Departamental** **Gestión Tributaria**	Identificaciones Generales sobre medidas de seguridad.
Dr. Fabián Altamirano **Jefe Departamental** **Jurídico**	Se han dado medidas generales
Ing. Leslie León **Secretaria Regional**	Se socializa a través del correo se entiende que todos conocemos

5. En los casos de infracciones a las normas de seguridad implementadas, ¿se han definido y aplicado sanciones por incumplimiento?

Tabla 26: Infracciones a las normas de seguridad

Variables	Nº	%
Si	3	33%
No	5	56%
N/A	1	11%
Total	9	100%

Gráfico 24: Infracciones a las normas de seguridad

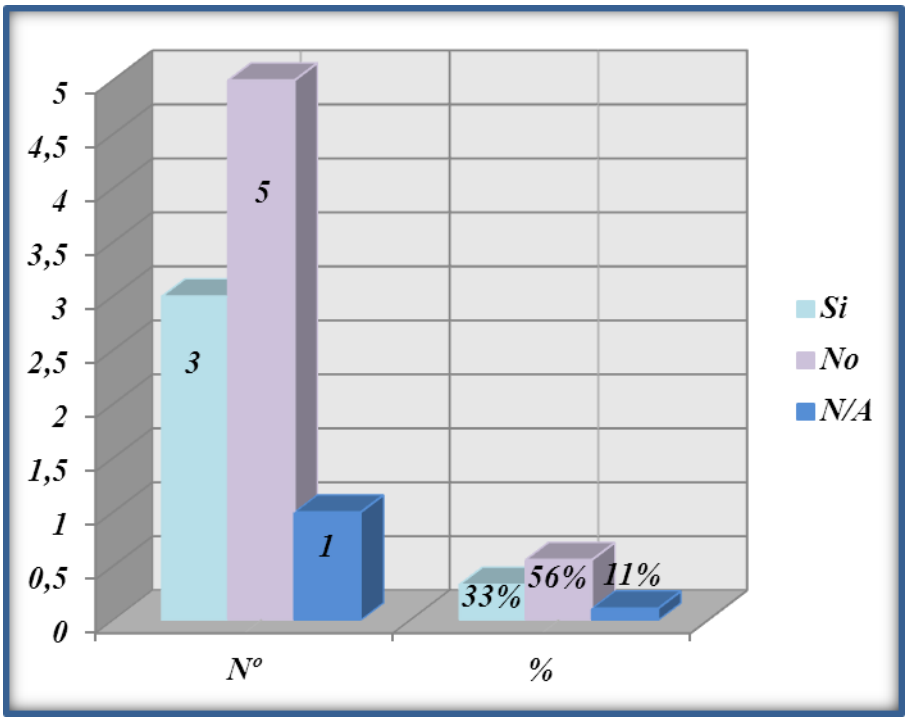


Tabla 27: Guía de entrevista pregunta 5

Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Si se han aplicado
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Porque no ha habido casos de infracciones
Ing. Leslie León **Secretaría Regional**	No ha tenido casos

6. **¿Ha solicitado, al responsable del proceso de control, en caso de haberlo, informes de cumplimiento de las seguridades implementadas?**

Tabla 28: Informes de cumplimiento de las seguridades implementadas

Variables	Nº	%
Si	1	11%
No	8	89%
Total	9	100%

Gráfico 25: Informes de cumplimiento de las seguridades implementadas

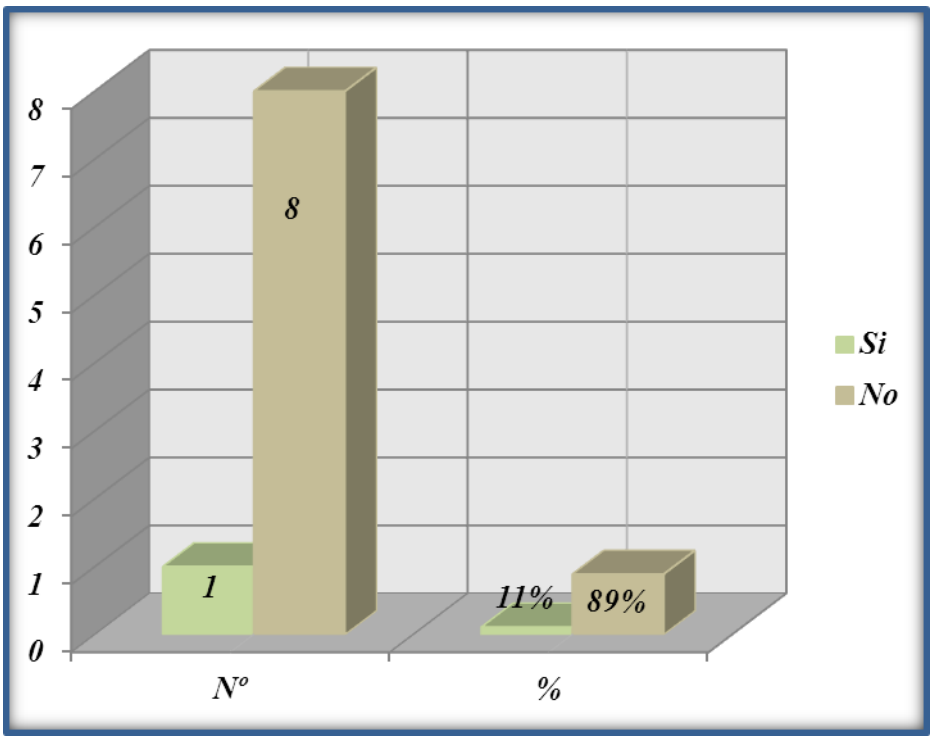


Tabla 29: Guía de entrevista pregunta 6

Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Son Monitoreos periódicos
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Se requería principalmente para control de impresiones
Dr. Fabián Mera **Jefe Departamental** **Gestión Tributaria**	Solicita en forma especifica por la información restringida que maneja pero no es oportuna

7. **¿Dentro de las seguridades implementadas, considera usted que se cuentan con adecuadas técnicas de alerta temprana para detección de riesgos?**

Tabla 30: Alerta temprana para detección de riesgos

Variables	Nº	%
Si	4	44%
No	5	56%
Total	9	100%

Gráfico 26: Alerta temprana para detección de riesgos

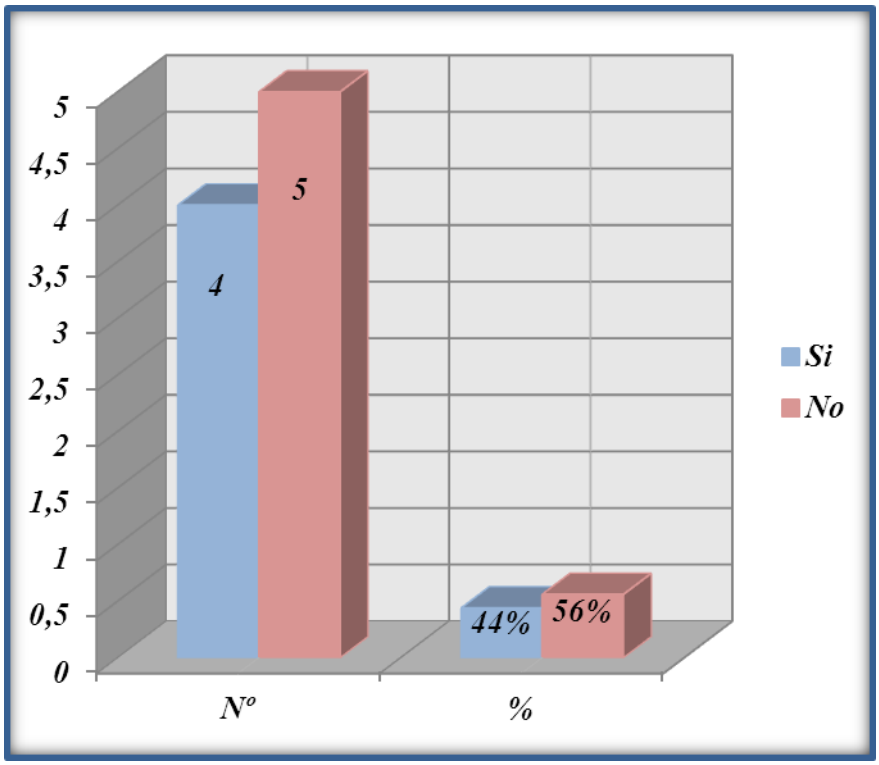


Tabla 31: Guía de entrevista pregunta 7

Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Existen pero no son suficientes
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Hay avisos en el Sistema de RUC, especialmente para minimizar el riesgo de errores con contribuyentes
Ing. Leslie León **Secretaría Regional**	Hay pistas de auditoría, el que exista previene acciones no permitidas
Eco. Jeannet Velastegui **Jefe Departamental** **Reclamos**	Si, sin embargo no son frecuentes, son esporádicos especialmente para seguridad personal

8. **¿Considera usted que el nivel de cultura de seguridad que maneja el personal es adecuado?**

Tabla 32: Nivel de cultura de seguridad

Variables	Nº	%
Si	2	22%
No	7	78%
Total	9	100%

Gráfico 27: Nivel de cultura de seguridad

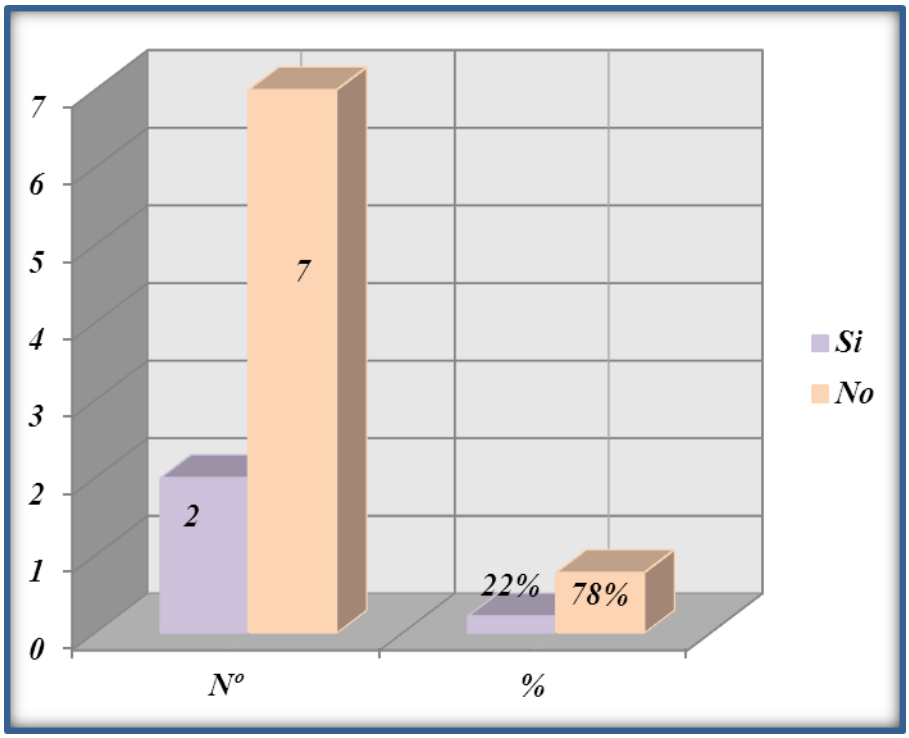


Tabla 33: Guía de entrevista pregunta 8

Entrevistado	Respuesta
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Debería haber controles diferenciados de acuerdo a la información que maneja cada departamento.
Dr. Fabián Mera **Jefe Departamental** **Gestión Tributaria**	Hay un sistema de cultura pero no es adecuado

9. **¿Considera usted que los controles y seguridades físicas y tecnológicas actualmente en uso son suficientes y adecuados?**

Tabla 34: Controles y seguridades físicas - tecnológicas

Variables	Nº	%
Si	5	56%
No	4	44%
Total	9	100%

Gráfico 28: Controles y seguridades físicas - tecnológicas

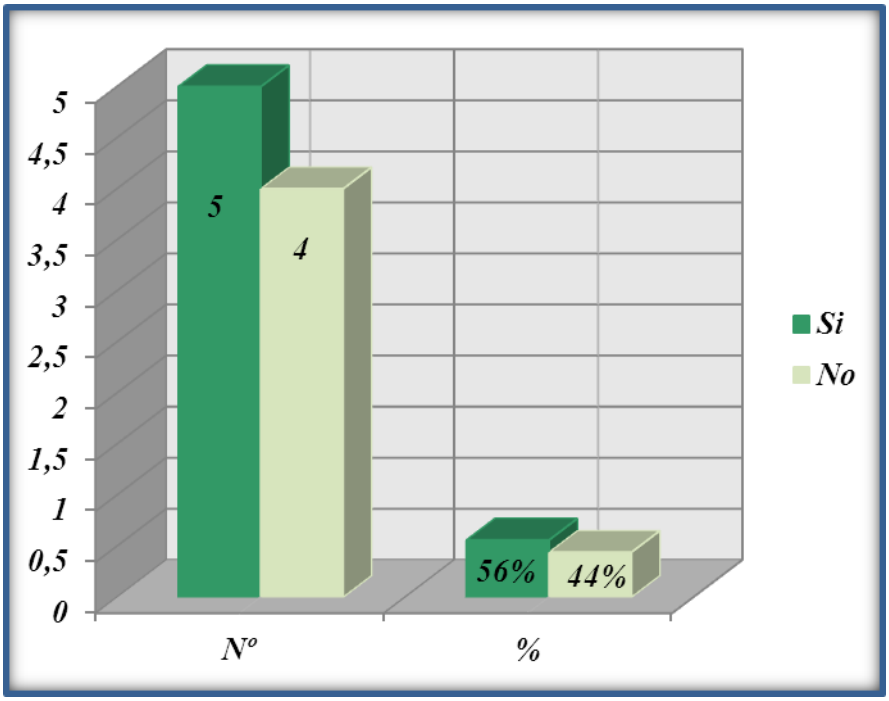


Tabla 35: Guía de entrevista pregunta 9

Entrevistado	Respuesta
Ing. MBA Tarquino Patiño **Jefe Administrativo Financiero**	Son adecuada pero no suficientes
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Son suficientes pero no adecuadas identificando la realidad de cada oficina del SRI.
Dr. Fabián Mera **Jefe Departamental** **Gestión Tributaria**	Considera que hay suficientes seguridades pero no se explota en su totalidad
Eco. Mateo Villacis **Jefe Departamental** **Planificación**	A profundidad no conocemos todas las seguridades
Dra. Viviana Paredes **Jefe Departamental** **Auditoria**	Sin embargo no se han realizado evaluaciones para verificar la suficiencia de los controles

10. ¿Se han realizado evaluaciones sobre la incidencia de un adecuado Plan de Seguridad Corporativa sobre el número de delitos o infracciones cometidas por el personal?

Tabla 36: Evaluaciones de un adecuado plan de seguridad

Variables	Nº	%
Si	1	11%
No	8	89%
Total	9	100%

Gráfico 29: Evaluaciones de un adecuado plan de seguridad

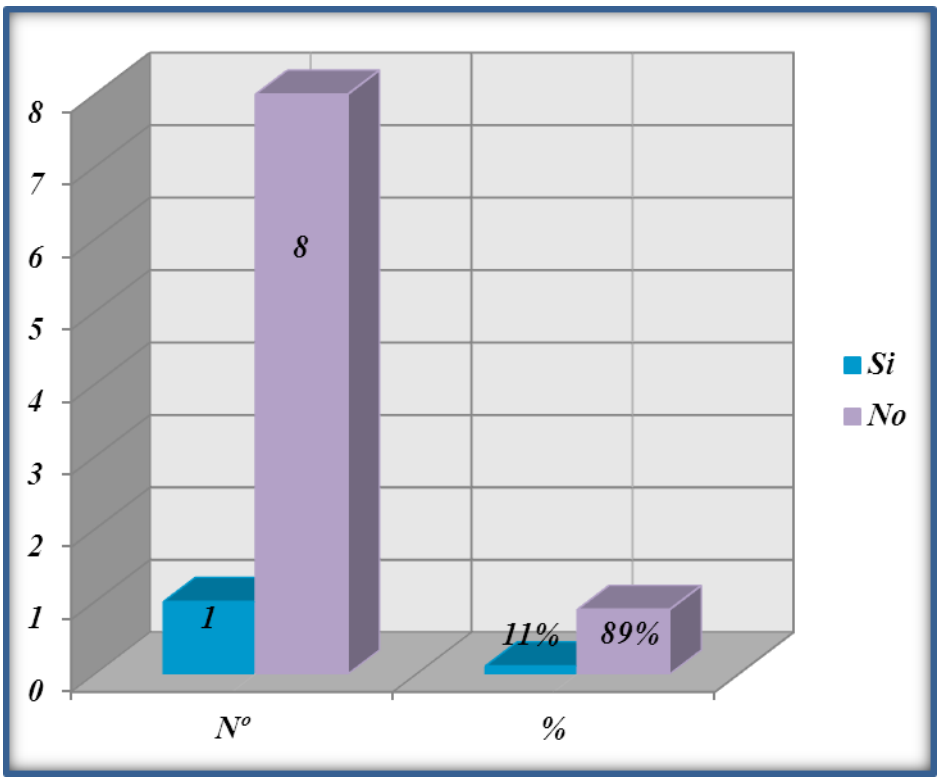


Tabla 37: Guía de entrevista pregunta 10

Entrevistado	Respuesta
Ing. Tannia Miño **Jefe Departamental** **Servicios Tributarios**	Se han realizado los pedidos respectivos
Eco. Jeannet Velastegui **Jefe Departamental** **Reclamos**	Cree que si por los correos recibidos respecto a esta información y las acciones realizadas.

Análisis de las entrevistas

Mediante las entrevistas realizadas se establecen que se han desarrollado procesos de Seguridad Corporativa en el SRI, se han realizado los pedidos respectivos, no se conoce a profundidad todas las seguridades, las mismas no se desarrollan en su totalidad, los entrevistados pusieron hincapié en desarrollar controles diferenciados de acuerdo a la información que maneja cada departamento.

4.2. Interpretación de datos

De los datos obtenidos de la encuesta se logro determinar el tema de seguridad corporativa en el SRI.

Con relación a la primera pregunta de la encuesta que trata sobre los controles implementados para la seguridad física de las instalaciones, de las personas encuestadas, el 31% contesta que Si conoce, el 69% No, es decir, que existe un alto porcentaje de desconocimiento sobre la seguridad corporativa en la institución que fue objeto de esta investigación.

Se determina en la segunda pregunta sobre la instrucción y las seguridades tecnológicas para el manejo de equipos de computación a su cargo, el 51% respondió Si, el 48% de los encuestados por el No, No responde el 1%; es preocupante que el 48% no tenga discernimiento sobre seguridad informática, es necesario poner énfasis en un buen manejo de la información, en instituciones como el SRI es vital que se tomen las medidas necesarias para evitar pérdidas de información o que la información personal de los usuarios caiga en manos equivocadas.

En la tercera pregunta, identificando a la Seguridad Personal como las medidas que permiten minimizar riesgos o vulnerabilidades sobre su integridad física: ¿Considera usted que existen adecuadas seguridades personales en su lugar de

trabajo?, de los encuestados el 33% contesta que Si, el 67% considera que No, del personal investigado se obtiene que no se han aplicado medidas preventivas para evitar riesgos en lugar de trabajo, es necesario concienciar sobre seguridad corporativa poniendo énfasis en estrategias con todos los departamentos.

En la cuarta pregunta, que menciona el caso de ausencia temporal en el lugar de trabajo, se investigó si los encuestados conocen sobre las seguridades que se debe aplicar, el 41% contesto Si, el 59% No, existe discernimiento, pero mas del 50% desconoce sobre las medidas a implementarse, los planes de seguridad internos no incluyen este tipo de temas o no se informa sobre sus contenidos.

En la quinta pregunta sobre la identificación clara de las áreas de acceso restringidas al público, el 73% contestó Si, en cambio el 27% No, los empleados conocen sobre las áreas restringidas, pero es necesario reforzar conocimientos con las personas involucradas en todos los departamentos del SRI.

En la sexta pregunta, sobre si son adecuadas las seguridades para salvaguarda de la información que manejan, el 54% respondió que Si, el 46% de los encuestados No, se concluye que existe una tendencia similar se considera en algunos casos que las medidas son adecuadas en otros existe una respuesta negativa, por ello es necesario desarrollar modelos para mejorar la capacitación del personal, sobre riesgos y seguridad corporativa.

En la séptima pregunta, que se refiere sobre si en alguna ocasión ha perdido información física o magnética importante en el desarrollo del trabajo, de los encuestados el 36% manifiesta que Si, el 64% contestó No, se ha presentado problemas de pérdida de información pero los mismos no son muy frecuentes ni preocupantes, a pesar de ello hay que optar por desarrollar para evitar pérdida de datos.

En la octava pregunta, que está relacionada con la séptima, los encuestados responden sobre el procedimiento a seguir para la recuperación de dicha información, en este caso el 4% manifiesta que Si, el 40% contesto No, y el 56% fue no aplicable, se concluye que existe un alto desconocimiento sobre el tema de un buen manejo de la información y como recuperarla, dentro del sistema de seguridad es necesario establecer parámetros de seguridad.

En la novena pregunta, ¿En caso de siniestros, que se detallan a continuación, conoce el procedimiento a seguir?, se encuestó sobre diversa clase, en el caso de terremoto, el 52% manifiesta que Si, el 48% de los encuestados contestaron No, es decir, es alto el índice de desconocimiento sobre las medidas de seguridad en el trabajo ante un terremoto,

Sobre incendios solo el 29% respondió que Si, el 70% optó por el No, solo 1% No responde a la pregunta, en el caso de este tema, es preocupante que no se conozca sobre las medidas que se deben tomar en el caso de incendios, es necesario establecer recomendaciones, se puede trabajar con otras entidades en configurar sobre la prevención y control de incendios

Otro tema analizado en la encuesta sobre siniestro fue inundación de los encuestados, el 11% responde Si, por el No el 87%, el 2% decide No responde, por lo cual es preocupante saber que no se conoce como actuar antes diversas clases de siniestros.

En el caso de erupción volcánica, el 51% de los encuestados respondió que Si, un 48% dijo que no sabía, el 1% No responde, existe conocimiento en % pero prolifera el desconocimiento sobre el tema tratado.

En la décima pregunta, acerca del conocimiento de los procedimientos a seguir para crear respaldos periódicos de la información que está bajo responsabilidad, el

35% manifiesta que Si, el 65% responde No, no existe manual de procedimientos para garantizar la seguridad de la información del SRI.

En la décima primera pregunta, que trata sobre si es necesario un adecuado programa de Seguridad Corporativa, que defina controles previos para minimizar los riesgos, como resultados se obtuvo, todos los encuestados contestaron el 100% contesto Si, existe la predisposición para implementar propuesta a favor de la seguridad corporativa.

A través de la entrevista se estableció que se han desarrollo planes de seguridad corporativas, los mismos no se encuentran actualizados y dirigidos a cada departamento del SRI.

4.3. Verificación de la Hipótesis

Sobre la base de la información obtenidos en la encuestas, para demostrar la hipótesis, se seleccionaron las preguntas número 1 y 3.

- ¿Conoce usted los controles implementados para la seguridad física de las instalaciones?
- Identificando a la Seguridad Personal como las medidas que permiten minimizar riesgos o vulnerabilidades sobre su integridad física: ¿Considera usted que existen adecuadas seguridades personales en su lugar de trabajo?

Planteamiento de la hipótesis

H0: "La insuficiente Seguridad Corporativa no impide la identificación en forma oportuna los riesgos en el Servicio de Rentas Internas Ambato"

0= E

H1: "La insuficiente Seguridad Corporativa es lo que impide la identificación en forma oportuna los riesgos en el Servicio de Rentas Internas Ambato"

$$\mathbf{0} \neq E$$

Estimador estadístico

Chi cuadrado

$$\mathbf{X^2 = \Sigma[\frac{(O-E)2}{E}]}$$

En donde:

$\mathbf{X^2}$ = Chi Cuadrado.

$\sum$ = Sumatoria.

O = Frecuencia Observada.

E = Frecuencia Esperada.

Nivel de significancia y regla de decisión.

$\alpha = 0.05$ (nivel de significancia) $1 - \alpha = 1 - 0.05 = 0.95$

gl = (c-1)(h-1)

Donde:

gl = grado de libertad

c = columna de la tabla

h = fila de la tabla

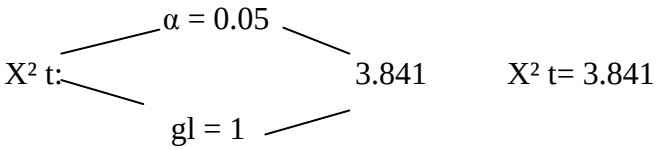
Para el cálculo del $\mathbf{X^2}$ tomaremos las preguntas 1 y 3 de las encuestas

Reemplazando tenemos:

gl = (2 – 1) (2 – 1)

gl = (1) (1)

gl = 1



g' ….. 0.05
1 ……3.841

Si X² c > a X² t= 3.841 se rechaza la hipótesis nula Ho y se acepta la hipótesis alterna H1

Cálculo de Chi Cuadrado (X² c)

De acuerdo al análisis de las respuestas se llega a la conclusión de que la Hipótesis se verifica, es decir:

La insuficiente Seguridad Corporativa es lo que impide la identificación en forma oportuna los riesgos en el Servicio de Rentas Internas Ambato.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Es necesario contar con planes de seguridad corporativa, son indispensables para garantizar medidas – procedimientos para la prevención de riesgo y crisis.
- La aplicación de Seguridad Corporativa no son prioritarios en las instituciones públicas existe deficientes mecanismos para garantizar controles informáticos efectivos.
- La implementación de un sistema de Seguridad Corporativa, fomenta la eficiencia y ayuda a garantizar la optimización de los sistemas, sub-sistemas, recursos, la fiabilidad de la información financiera y el cumplimiento de las normas vigentes.
- La gestión corporativa es alta gravitación para la consecución de los objetivos institucionales, cada vez es mayor la necesidad de aplicarlo, lo que hace que se justifique ventajosamente su aplicación en la sede central, sucursales y agencias del SRI
- Asegura un seguimiento adecuado para constatar si las políticas y actividades de control son obedecidas por los directores, gerentes, funcionarios, trabajadores y usuarios. Lo que conllevaría a la optimización institucional y un proceso de mejoramiento continuo, con todo lo cual se puede competir ventajosamente en la coyuntura actual.

- La seguridad es un proceso continuo, no se pueden establecer unas medidas de seguridad extremas para mantener la integridad de los datos y procesos de la empresa y luego, olvidar que es necesario realizar un seguimiento continuo de las medidas implantadas, actualización de Software, revisión periódica del Hardware, etc.
- El personal tiene una buena conciencia de lo importante que es la seguridad corporativa para la Institución, por lo cual demanda su implementación.
- A lo largo de la realización del proyecto se ha comprobado en numerosas ocasiones que el personal no son conscientes de lo importante que es la seguridad informática para su proceso de negocio y lo vulnerable que es a posibles pérdidas de información.
- La naturaleza de las amenazas que pueden afectar a una organización han cambiado.
- La naturaleza de las amenazas han cambiado, los creadores de virus ya no tratan de propagarlos rápidamente y conseguir con ello un "record" de infecciones y cierta notoriedad sino que ahora tratan de colarse en sistemas para robar el mayor número de información posible sin ser detectados.
- La institución debe reforzar las seguridades para no estar desprotegida ante posibles ataques informáticos
- Ejecutar procesos permanentes de control para evitar una desactualización de los sistemas de seguridad con los que ya se cuenta y por mejoras que se puedan implantar en los sistemas.
- Se ha identificado el desconocimiento de las seguridades implementadas por parte del personal que integra la Institución y la ausencia de una sólida cultura de seguridad.

5.2. Recomendaciones

- Involucrar a los colaboradores en el sistema de gestión integrado para facilitar su uso y entendimiento, estableciendo para ello planes de socialización de las seguridades implementadas.
- Promocionar y concientizar al personal sobre las normas de seguridad informática y su actualización periódica para garantizar que no exista perdidas de información
- Aplicación de programas de gestión corporativa, que englobe sistemas de seguridad personal, acceso a áreas restringidas, seguridades tecnológicas, seguridades físicas de las instalaciones, siniestros, inventario de los riesgos.
- Procurar la generación de un ambiente y cultura de seguridad sólida que se irradie en toda la Institución.
- Incentivar a los colaboradores para que realicen sugerencias con el fin de mejorar los procesos.
- Realizar auditorías periódicas, recomendablemente bienales, del nivel de seguridad en que se encuentra la empresa.
- Continuar con los procesos permanentes de actualización de todo el Software de la Institución: antivirus, Sistema Operativo, Software de gestión, principalmente, e involucrar a todo el personal en el conocimiento de estos trabajos.
- La aplicación de la seguridad corporativa, con la incorporación de prácticas modernas exitosas permitirá asegurar que las políticas, estrategias, tácticas, procesos y procedimientos vigentes se adecuen a las necesidades de los usuarios elevando su nivel de satisfacción con el servicio recibido.

CAPÍTULO VI

6. PROPUESTA

6.1. Datos Informativos

- ***Titulo***

Diseño de un Sistema Integral de Seguridad Corporativa que constituya un control previo en Auditoría Forense

- ***Beneficiarios:***

Los beneficiarios de la propuesta son:

- Directivos del SRI
- Personal que labora en el SRI
- Comunidad en General

- ***Ubicación***

Ambato, centro de la ciudad

- ***Tiempo estimado para la realización***

Doce meses

- ***Equipo Técnico Responsable*:**

La Autora del trabajo de grado Dra. Mercy Solis

- ***Costo:***

El costo aproximado del proyecto es de $2.000,00 (dos mil dólares americanos)

6.2. Antecedentes de la propuesta

Los sistemas informáticos de las empresas se encuentran repletos de soluciones de seguridad para proteger la información corporativa. Sin embargo, una Política de Seguridad mal definida o inexistente, entornos tecnológicos heterogéneos, instalaciones mal planificadas o personal técnico sin formación específica determinan un escenario deshilachado y mal engranado. Es necesario complementar las herramientas de seguridad con sistemas que las controlen e integren desde un punto de vista lógico.

Para determinar el desarrollo de la propuesta se investigó a través de la encuesta y la entrevista realizada que existe un plan de seguridad de bienes y personas realizado hace dos años, el mismo no se ha actualizado sobre riesgos físicos, por ello es necesario implementar un sistemas de seguridad corporativa que englobe todo los temas necesarios, normas y medidas para garantizar la seguridad.

Se determinó su necesidad en base a la décima primera pregunta, que trata sobre si es necesario un adecuado programa de Seguridad Corporativa, todos los encuestados contestaron el 100% que Si

6.3. Justificación

Identificar, mitigar y administrar efectivamente riesgos y vulnerabilidades que puedan amenazar la seguridad de la empresa, la capacidad de recuperación y la supervivencia de la organización. Esto implica una serie de acciones coordinadas y orientadas a un objetivo específico utilizando sus cuatro recursos o activos principales: recursos humanos, financieros, administrativos y operativos

El sistema debe actualizarse con periodicidad, estar dotados de suficientes recursos y determinar los mecanismos para saber qué se ha incumplido. Esta es la parte reactiva de la seguridad.

La seguridad es un elemento imprescindible de la reputación de las empresas. Un error, como la pérdida de información clave, puede acabar con el buen nombre.

La falta de disponibilidad de servicios críticos ante eventos contingentes, entre otros, alertan de la importancia de la seguridad de la información dentro del entorno empresarial, cada vez más interconectado y abierto a sus socios, proveedores y clientes.

Estos incidentes de seguridad demuestran que el enfoque de seguridad de la información sigue siendo en la actualidad eminentemente reactivo y centrado exclusivamente en los sistemas de información. Sólo factores externos como el normativo y regulatorio ponen un punto de presión y sensibilización en las organizaciones.

Seguridad Corporativa es más que cámaras de vigilancia o personal de seguridad armados. Su efectividad se basa en la lógica y en el correcto manejo de información (prevención) antes que en la fuerza bruta y capacidad de fuego (reacción). Se ha convertido en una herramienta clave para apoyar el logro objetivos estratégicos del negocio. Es defender a la empresa contra potenciales

fugas y pérdidas que, de hacerse realidad, pueden generar una crisis que signifique el inicio de una pérdida de imagen y competitividad, hasta llegar a su extinción.

6.4. Objetivos

General

Promover la ejecución del proyecto para la implementación de un Sistema de Integral de Seguridad Corporativa que constituya un control previo en Auditoría Forense, con el apoyo de las principales autoridades del SRI.

Específicos

- Socializar la propuesta con las autoridades del SRI, los empleados que propicie el apoyo institucional y económico para la ejecución de actividades previstas en el sistema de seguridad corporativa.
- Desarrollar el plan operativo de ejecución de la propuesta que permita la consecución de metas y objetivos a corto y mediano plazo.
- Diseñar el Sistema Integral de Seguridad Corporativa en el SRI, en base a consensos y criterios entre autoridades, empleados y clientes.

6.5. Análisis de Factibilidad

Política

Es factible la realización del proyecto, para su desarrollo se buscará el apoyo de especialistas en el desarrollo de sistemas de seguridad corporativa, se pedirá el consentimiento y aprobación de las autoridades y de los empleados, se establecerán líneas estratégicas y políticas para garantizar la seguridad, todo enmarcado en base a los objetivos y metas del SRI (Servicio de Rentas Internas).

Sociocultural

El sistema de seguridad corporativa, busca mejorar lo servicios en el SRI, la prevención de riesgos, motivando a la confianza hacia las entidades pública, mejorando los procesos organizaciones en temas de seguridad, garantizando capacitación y gran espíritu de trabajo, es necesario en cada ámbito de la propuesta respetar y fomentar la diversidad en términos de cultura, sexo, edad, raza, condición social e ideología política

Tecnológica

Se utilizará la mejor tecnología para el desarrollo de un sistema de información sobre seguridad, capacitando al personal, se mejorará procesos para garantizar seguridad informática, evitando pérdidas de datos esenciales para la institución y mal manejo de los equipos de computación. Se utilizará programas informáticos actualizados, y sistemas de protección innovadores.

Organizacional

Una gran parte del éxito de la propuesta se basará en el elemento humano que interactúa con los demás elementos que lo integran, como son procesos, controles, normatividad y sistemas electrónicos.

La propuesta se realizará en base a una recopilación de información sobre los riesgos de la empresa, con el involucramiento de expertos en base a una planificación sistematizada, en base a los objetivos de la propuesta, desarrollando las gestiones necesarias para que el personal del SRI y las autoridades apoyen su diseño y ejecución.

Equidad de Género

El sistema será dirigido tanto al personal femenino como masculino del SRI (Servicio de Rentas Internas), es decir, se trabajará con todos los Departamentos, el sistema de seguridad corporativa estará al alcance de todos los involucrados y los beneficiarios de la misma.

Ambiental

No causará ningún impacto ambiental, se establecerán normas de seguridad ambiental para un buen uso de la energía, evitar contaminación y capacitar sobre siniestros como terremotos, erupciones volcánicas, se ahorrará recursos reciclando papel, no se requiere estudios ambientales.

Económico – Financiero

El proyecto se desarrollará con el apoyo de la entidad beneficiaria y otras entidades que apoyen estas iniciativas, con recursos para su implementación definitiva.

Legal

No hay ningún impedimento legal para la realización de la propuesta.

6.6. Fundamentación Científico – Técnica

Nivel de Seguridad:

El medio en el que los empleados públicos desarrollan su actividad profesional, está permanentemente sometido a un conjunto de amenazas que gravitan sobre las personas, los bienes, los valores y el normal funcionamiento de los servicios.

La sociedad actual ha incrementado considerablemente la probabilidad y potencialidad de esas amenazas por causas tan diversas como el empleo de poderosas fuentes de energía, la aplicación de avanzados procesos tecnológicos, el desarrollo de macro industrias, el sobredimensionamiento de los almacenajes, la evolución de los transportes y otros factores diversos.

Obvio es decir que la sociedad moderna tiene que hacer frente a la situación de inseguridad expuesta y, en el caso de la empresa, ello es siempre responsabilidad y competencia de la alta dirección. A este nivel, resulta imprescindible conocer la problemática de seguridad del conjunto empresarial, lo que determina la necesidad de efectuar un estudio de seguridad o, al menos, una auditoria competente.

El resultado será un conocimiento preciso de los diversos riesgos y de las diferentes soluciones posibles, así como del coste de cada una de ellas. Sobre la base de estos elementos, la dirección del ORGANISMO puede ya plantear los objetivos que resuelvan, en el espacio y en el tiempo, la problemática de seguridad existente, lo que se traducirá en el establecimiento de unas prioridades y unos plazos.

La dirección de seguridad, para la consecución de esos objetivos en el orden y en los tiempos requeridos, determinará los recursos humanos y presupuestarios existentes así como las necesidades, tanto organizativas como los medios materiales.

El desarrollo descrito constituye una parte del denominado proceso de decisión, cuya exposición completa cabe establecer en cinco fases, correspondientes a las diferentes actuaciones de la Dirección del ORGANISMO y de la dirección de seguridad.

- La primera fase la forman la determinación, análisis y valoración de los riesgos, integrantes del estudio o de la auditoria de seguridad, que la Dirección del ORGANISMO habrá encargado realizar.
- La segunda fase la constituye el establecimiento, por parte de la Dirección, de los objetivos así como las prioridades y plazos para su consecución.
- La tercera fase corresponde a la dirección de seguridad y comprende el análisis, determinación y presentación de los recursos disponibles- humanos y presupuestarios- y las necesidades- organizativas y materiales para la consecución de los objetivos.
- La cuarta fase, representada por el tratamiento de los riesgos, constituye el acto de decisión en la aplicación de las diferentes soluciones posibles y compete, obviamente, a la Dirección del ORGANISMO, bajo el asesoramiento y propuestas del director de seguridad.
- La quinta fase comprende la actuación sobre aquellos riesgos que se haya decidido su eliminación o reducción. Consistirá en la elaboración, implantación y gestión de los correspondientes planes de prevención y protección.
- Si a estas fases se la somete a la estructura que tiene un Ministerio, Consejería y/o un Organismo Público, se harán- y de hecho se hacen- interminables, produciendo la conocida situación de problemas que nunca se solucionan, soluciones que tardan meses en llegar o se atiende al problema porque se ha producido un acto antisocial que obliga a intervenir sin la preceptiva auditoria de seguridad, solo para contentar a los electores.

Evaluación del riesgo forense

Según **Jorge Badillo (2008: 20)**, el auditor debe evaluar el riesgo de distorsión material que el fraude o error pueden producir en los estados financieros y debe indagar:

- Existen fraudes o errores significativos que hayan sido descubiertos.

- Visualización de debilidades del diseño de sistemas de administración.
- Presiones inusuales internas o externas sobre la entidad.
- Cuestionamientos sobre la integridad o competencia de la administración.
- Transacciones inusuales.
- Problemas para obtener evidencia de auditoría suficiente y competente.

Establecimiento de áreas de riesgo

Una vez que han sido identificadas las áreas, éstas deben ser priorizadas a fin de considerar su vulnerabilidad, para lo cual se puede utilizar en cierta medida el análisis sistemático de riesgo (método helvético) y que permite puntualizar las auditorías en áreas establecidas como de mayor riesgo, las cuales se compensan al ser comparadas frente al sistema de Control Interno, que permite determinar hasta que medida el sistema compensa o contrarresta las amenazas de fraude.

Para realizar este diagnóstico, el auditor consultará documentación referente, como son los informes de auditorías anteriores del revisor fiscal, de auditorías externas, de otros entes de control, denuncias y quejas, así como los procesos que se adelanten contra la institución.

Análisis de riesgos

El análisis sistemático de riesgos es un enfoque estructurado que ayuda al auditor y, por consiguiente, a la administración a tomar decisiones fundamentadas. Lo básico es contar con una matriz donde se puedan resumir los resultados de la evaluación inicial.

El primer criterio es tener en cuenta los sectores de examen que hacen alusión a las tareas específicas que son llevadas a cabo en la Entidad o en una unidad orgánica En la matriz éstas ocupan las filas. Luego, se establecen los criterios de

evaluación, los que pueden ser numerosos, entre ellos se presentan: Sistema de Control Interno, Complejidad de las tareas. Ponderación financiera, Modificaciones y Observaciones.

Los criterios principales se subdividen en Criterios Parciales. A los cuales se pueden asignar valores de ponderación:

3 = Ponderación alta,
2 = Ponderación media,
1 = Ponderación baja o niveles de Evaluación:

Bajo=buen grado de cumplimiento
Medio= Grado de cumplimiento suficiente.
Alto- Grado de cumplimiento deficiente

Gestión empresarial de Seguridad

Los tres elementos clave de la Gestión Estratégica Empresarial

Los incesantes y precipitados cambios en la tecnológica, conjuntamente con la disminución en el tiempo de vida de los bienes y servicios, los constantes cambios en los hábitos de los consumidores; los cuales poseen cada día más información y son más rigurosos

Esto se suma a la inclemente competencia a nivel global que exige a las empresas mayores niveles de calidad, acompañados de mayor diversidad, menores costos y tiempo de respuestas, requieren todos ellos de la aplicación de métodos que en forma integral permitan hacer frente a los diferentes retos que se presentan en nuestra actividad en el día a día.

Joel Barker, en su libro "Paradigmas", menciona los que, para él son los tres elementos claves de la Gestión Estratégica Empresarial, para quienes deseen ser competitivos hoy en día. Estos son: Excelencia, Innovación y Anticipación.

Utilizando este punto de vista, y llevándolo al mundo de la seguridad, podemos decir que son los factores críticos del éxito de nuestra labor, toda vez que no debemos inventar la rueda, pues todo ya está inventado. Con esto quiero iniciar la definición, desde mi percepción, de cada uno de estos elementos claves.

Excelencia:

Hace referencia a que siempre encontraremos a alguien con quien compararnos y que realiza la misma actividad nuestra, siendo los primeros en ella, lo que nos obliga a iniciar nuestro trabajo por lo menos en este punto.
Así, lo que hacemos con posterioridad a este inicio es el mejoramiento de nuestros productos, buscando mejorar lo que para muchos pueda ser inmejorable.

Ejemplos pueden existir, pero el que más me gusta hace referencia a la "gerencia japonesa", que se orienta hacia la calidad total. Entre los componentes que posee esta excelencia, está en primer lugar y como base de partida, la calidad humana de vida de las personas que desarrollan la labor de seguridad.

Sumado a esto se encuentra la calidad del proceso, hecho este que como todas las actividades en cualquier entorno lo realizan las personas, y por ende debemos realizar una reingeniería en la forma de pensar de nuestros hombres de seguridad, pues solo a través de ellos lograremos enfrentar los retos de la excelencia.

Cuando se habla de calidad humana de vida, se habla de desarrollo personal, autoestima, visión personal y profesionalismo. Sin que el profesionalismo signifique un sin número de títulos colgados en las paredes de nuestras oficinas, pues este profesionalismo está orientado a entender nuestro rol dentro del

escenario empresarial donde prestamos nuestro servicio de seguridad, que incluye el qué, el como, el por qué y el para qué.

Esto nos lleva entonces a decir que la formación y el aprendizaje de los hombres de seguridad juega papel importantísimo en el desarrollo de equipos competitivos, sin olvidar que un equipo aprende a través del aprendizaje de los integrantes del mismo, pero que esto per se no es suficiente se necesita de la retroalimentación de las partes para lograr un aprendizaje en conjunto que genere valor agregado.

Es por esta razón que cada vez que vinculamos a nuestras organizaciones un hombre de seguridad se le debe incitar a que desde el momento que se "sube al tren" deberá sincronizarse y alinearse con los objetivos estratégicos trazados por la organización. Pues bien, el reto final en busca de la excelencia esta en el deseo de los integrantes del equipo de seguridad en aprender a aprender con el único propósito de buscar ser competitivos.

Cuando se habla de calidad en los procesos de seguridad, hablamos de mejoramiento continuo e implícitamente hablamos de quien hace las cosas eso es el factor humano, a quien en muchas ocasiones no se les escucha y se pierden por ende muchas iniciativas que contribuirían al mejoramiento de un procedimiento de seguridad, a optimizar recursos y a mejorar los costos.

No podemos olvidar que la seguridad como cualquier otra actividad comercial trabaja en función de un cliente, ya sea de carácter interno o externo. Por consiguiente, debemos estar preparados para identificar las necesidades de ese cliente y buscar de forma acertada la satisfacción de la misma.

Innovación:

Este segundo elemento es de suma importancia en las personas de seguridad, pues debe convertirse en un estilo de vida.

Como ejemplo es bueno citar el Kaizen, que significa “La mejora que involucra a todos: alta administración, gerentes y trabajadores”.

Así, el ejercicio de innovar esta siempre unido a la parte derecha de nuestro cerebro. Tal vez la pregunta para iniciar es ¿funciona el mío?, y la respuesta es un rotundo si, pues todos los seres humanos poseemos esa cualidad. El problema es lograr el desarrollo de la misma.

En cuanto a los hombres de seguridad siempre será bueno estarles preguntando que podrían mejorar en su puesto de trabajo para lograr un óptimo desempeño de sus labores y conseguir que ese aporte cree sinergias al interior de la organización que recibe nuestros servicios.

El problema generalmente con la innovación radica en el hecho de que a muchos de nosotros nos da miedo que alguien nos diga que estamos locos o salidos de la realidad, lo cual genera la primera barrera de expresión cuando de innovar se trata; pero si nos referimos a la historia, veremos que son muchos los casos de los locos que hoy son padres de algún invento que revolucionó el mundo, lo que indica que son esas ideas las que crean nuevos productos.

La mayor parte de los problemas de la innovación en seguridad sin duda se derivan del hecho de que no somos capaces de enfrentar aquellos paradigmas que subsisten en el medio y decidimos no decir nada por miedo de correr el riesgo de ser rechazado.

El verdadero problema de buscar la innovación en seguridad es que no hemos aprendido a identificar lo que nuestro cliente necesita y ofertamos productos que generalmente todos los proveedores ofrecen sin realizar los ajustes necesarios para el cliente que solicita el servicio, pues si bien la seguridad es un lenguaje universal, las organizaciones poseen sus propios problemas originados en cada

uno de sus procesos, lo que hace que ninguna organización se parezca a otra.

Cuando se logra la flexibilidad en los paradigmas hemos dado un paso hacia adelante que muy seguramente ayudará de forma activa en la búsqueda de nuevas ideas para la solución de muchos de los problemas que constantemente estamos enfrentando en la seguridad.

No podemos olvidar que cuando se genera una fisura en los esquemas de seguridad, necesitamos de nuestro primer elemento de seguridad que es el ser humano y si escuchamos a los que realizan el trabajo día a día muy seguramente encontraremos la solución más rápido de lo que esperamos.
Pero seguramente será preciso cambiar nuestra forma de ver las cosas, no ser tan ingenuos de creer que todo lo sabemos y que somos producto terminado, pues esto sería un pecado capital cuando de innovar se habla, pues siempre existirán cosas que mejorar.

Todo esto obliga a que el hombre de seguridad siempre esté buscando ser un líder en cada una de las actividades que debe asumir en el entorno organizacional.

Anticipación:

El último elemento de esta reflexión hace referencia al hecho de que el hombre de seguridad debe ser proactivo, que significa estar antes de que sucedan los acontecimientos, identificar lo que nos puede ayudar a ser competitivos en las organizaciones del futuro o mejor aun forzando situaciones que en el futuro pueda controlar basado obviamente en la mejor herramienta de seguridad, que es el análisis de riesgos.

Siempre que se habla de anticipación también se está hablando de las tendencias que se generan en los entornos donde laboramos, lo cual hace necesario volverse

un estudioso de las tendencias que en el mundo moderno ayudan de forma constante en la toma de decisiones.

Según **Diofanor Rodríguez (Internet: 2011),** cada vez que realizamos estudios juiciosos de las tendencias del mercado, de los modus operandi de los delincuentes, de la forma como los fraudes y los hurtos mutan hacia el ciberespacio, estamos tratando de buscar de forma anticipada cual será nuestra nueva defensa.

De la misma manera estamos ayudando a la organización para la que trabajamos a cambiar sus políticas de seguridad, sus procesos de funcionamiento y evitando poseer perdidas que al final afecten la continuidad del negocio.

La Seguridad basada en el valor

Para los directivos de seguridad corporativa, el foco de su tarea se desplaza desde el combate al delito, hacia el agregado de valor a la organización

El rol del directivo de seguridad va cambiando a partir de los cambios que deben enfrentar las organizaciones en las que trabajan. Se debe rediscutir las bases para los nuevos criterios corporativos de seguridad, la formación requerida para desempeñar este nuevo rol del directivo de seguridad, y poner el foco de su tarea en el agregado de valor a la organización.

Organización y agregado de valor

Toda organización existe para agregar valor para sus clientes, accionistas, colaboradores y la comunidad en su conjunto. En un momento de dura competencia, globalización y concentración de negocios, el imperativo empresario es crear ventajas competitivas y generar más valor que las empresas rivales, en un ambiente empresarial en continua reconfiguración.

Como lo demostrara Michael Porter en los años 80, las ventajas competitivas de una organización se encuentran en el modo en que realiza sus actividades: comprar mejor, tener mejor logística o un marketing de mayor calidad, etcétera, y con frecuencia, no pueden ser bien comprendidas analizando a la empresa como un todo. Para lograrlo, Porter diseñó el modelo de Cadena de Valor, que permite desagregar la actividad total de la empresa en actividades individuales diferentes, lo que permite comprender los costos de la empresa, y hallar fuentes de diferenciación y ventaja.

El Sistema de Valor combina la cadena de valor propia con las de los proveedores, canales de distribución y clientes, considerando que el producto de la empresa es parte de la cadena de valor del cliente.

Componentes de la cadena de valor

Según el Prof. Porter, una empresa, posee dos clases de actividades: Las actividades PRIMARIAS (logística interna, producción -operaciones-, logística de salida, marketing y ventas y servicio), y las actividades de APOYO (abastecimiento, desarrollo de tecnología, recursos humanos e infraestructura)

Un análisis cuidadoso de la cadena de valor brinda la ocasión de volver a pensar el papel de las actividades tradicionales. Por ejemplo en muchos negocios, tales como el monitoreo de alarmas, puede usarse el entrenamiento y reentrenamiento de clientes como herramienta de marketing.

Muchas veces, la misma función puede hacerse de distintos modos. ¿Cuáles son? ¿Cuánto cuesta cada uno? ¿Qué valor agrega cada uno al cliente? En otras ocasiones, puede mejorarse el desempeño en las actividades directas, por ejemplo operaciones o servicio, introduciendo mejoras en las indirectas, por ejemplo en capacitación o infraestructura.

Eslabones de valor

Llamamos eslabones a las relaciones entre distintas actividades de la cadena de valor. En ocasiones, por ejemplo, no tenemos problemas en logística, sino en el modo en que se relacionan logística y operaciones.

Es particularmente valioso concentrarse en el análisis de los ESLABONES VERTICALES, las relaciones entre nuestra cadena de valor y la de nuestros proveedores y clientes.

El análisis de eslabones verticales no es un "juego de suma cero". No es que cuando nosotros ganamos algo, ellos lo deben perder. En ocasiones ambas empresas pueden ganar.

El análisis del sistema de valor, la relación entre la cadena de valor propia y la de los clientes, es extremadamente importante. Y cada punto de contacto entre ambas, que da lugar a lo que Ian Carlzon llama "momentos de la verdad", puede ser una fuente de diferenciación.

Brinda la oportunidad de CREAR MÁS VALOR

a. Disminuyendo los costos
b. Aumentando el desempeño
c. Creando alguna ventaja competitiva, para la empresa o el cliente

Finalmente, el separar las actividades que realiza la empresa para analizarlas individualmente, brinda oportunidades de mejorar la calidad con que se las realiza, hallar modos de hacerla mejor o de agregar más valor para el cliente... o de dejar de hacerla si encontramos actividades que son parte de la rutina pero ya no agregan valor.

Seguridad y valor

La Seguridad es una relación dinámica entre tres elementos:

- Un valor,
- Un riesgo o agente agresor y
- Un agente protector.

Si no hay valor, no hay nada que proteger. Y en este esquema la seguridad, comprendida como la salvaguarda de propiedades, bienes y personas, es una función corporativa esencial.

Las demás funciones corporativas (dirección, manufactura, etcétera) no pueden desarrollarse sin Seguridad, pero pese a ello, ¿dónde hallamos a la seguridad corporativa en el modelo presentado?

Aquí comienza lo interesante de la discusión, ya que desde el punto de vista de la organización, el objeto de la Seguridad corporativa no es la protección en sí misma, sino la contribución que la seguridad puede aportar a la empresa en términos de beneficios tales como mejoras en su posición de mercado, y libertad de acción y disponibilidad de bienes y productos.

Este concepto suele chocar de lleno con las ideas de algunos responsables corporativos de seguridad. Los profesionales con mentalidad operativa, ponen el foco de su tarea en la calidad de las operaciones. Pero la compañía espera que el foco de la tarea del responsable de seguridad no esté solo en evitar delitos o pérdidas sino, de modo más abarcativo, en agregar valor para el negocio.

Esto implica que los criterios de Seguridad deben estar integrados a la toma de

decisiones en todas las áreas corporativas, tal como ocurre con los criterios administrativos, financieros, operacionales y de otros tipos.

Seguridad basada en el valor

Esto representa un desafío para el profesional de seguridad, ya que los criterios de seguridad ahora deben basarse en el valor, y el responsable de la función de seguridad debe preguntarse de modo continuo ¿qué es crítico, para este negocio y en esta situación específica

Y cuando el responsable de seguridad recomienda realizar inversiones para mejorar el nivel de seguridad de la organización, incorporar más personal, etcétera, ¿puede sustentar estas recomendaciones en criterios gerenciales basados en el valor para el negocio? Muchas veces no puede, o no sabe hacerlo.

Para desempeñar este nuevo rol, basado en el valor, también se requiere una nueva formación profesional. La antigua formación, centrada en habilidades operativas, no alcanza. Se requiere conocimientos del "core" del negocio, de finanzas y manejo de presupuesto, habilidades de negociación, etcétera, y entrenarse en la toma de decisiones basada de seguridad basadas en el valor para su organización.

Incluso en las propias operaciones, ha cambiado la capacitación mínima que las empresas requieren para su directivo de seguridad. La formación requerida va más allá de la capacidad de diseñar el dispositivo de protección, o de ser capaz de confeccionar un Estudio de Seguridad en forma autónoma. Hoy se requiere que el directivo de seguridad domine múltiples temas vinculados con el manejo de crisis, prevención de pérdidas, planes de emergencia, análisis de amenazas y su impacto en el negocio...

Con los conocimientos no alcanza

Según **Edgardo Frigo (Internet: 2011),** la organización no sólo busca personas que tengan los conocimientos necesarios, sino mucho más.

- Los conocimientos brindan el "saber cómo se hace".
- La competencia indica que el profesional "puede hacer"
- El desempeño es lo que el profesional realmente hace.

Lo que buscan las mejores empresas son profesionales de seguridad de alto desempeño: que sepan cómo agregar valor al negocio, que puedan hacerlo, y lo hagan en su tarea cotidiana. Por ello, las actividades de formación profesional deben centrarse en mejorar el desempeño real de los Colegas, no solo en sumar conocimientos y diplomas.

Concepto de Sistema

Tomamos el concepto de sistema que lo define como un todo unitario, organizado, compuesto por dos o más partes y delineado por los límites identificables expresamente de un entorno o de un suprasistema. En la gestión se lo define como el "conjunto de elementos mutuamente relacionados o que actúen entre sí".

Cada sistema se encuentra delineado por los límites que lo separan o lo interrelacionan con los restantes. A su vez toda organización está constituida por varios sistemas individuales mutuamente interactuantes. La adecuada concatenación e interrelación de los diversos sistemas hará que cada organización particular cumpla eficazmente con la misión para la cual se concibió.

Cuando se constituye un sistema existen tres opciones:

a) dejar que el sistema opere por sí solo y no prever las fallas que pueda llegar a tener,
b) dejar que el sistema opere por sí solo y prever las fallas que pueda llegar a tener
c) ajustarlo y adaptarlo constantemente, autosostenido.

La tercera opción es la que se ha seleccionado en los modelos de gestión aplicables en el marco de las normas ISO de la familia 9000, de la familia 14000 y de las normas OSHAS 18000.

En el caso de los sistemas integrados de gestión la meta fundamental es lograr eficiencia en todos los aspectos relacionados con la organización.

Aspectos Comunes a los Diferentes Sistemas

Todos los sistemas a los que se hará referencia tienen una serie de aspectos en común que son aquellos que permiten estudiarlos en forma uniforme y que permiten integrarlos a los efectos de su gestión.

Estos aspectos son, entre otros:

- establecer una política
- fijar objetivos definir responsabilidades y autoridades
- efectuar la documentación de los procesos, actividades o tareas a realizar y mantener dicha documentación controlada
- planificar las actividades y tareas a llevar a cabo para lograr los objetivos establecer procesos clave

- efectuar mediciones y seguimiento o monitoreo de procesos, actividades y tareas, llevar registros como evidencia de las actividades ejecutadas y controlar la gestión de los mismos
- tomar precauciones para controlar aquellos resultados o procesos que no satisfacen las especificaciones
- tener prevista la toma de acciones correctivas y preventivas cuando alguna situación no funciona de acuerdo a lo planificado
- efectuar la evaluación del desempeño del sistema a través de auditorías
- revisar el sistema en forma periódica por parte de la dirección

Empleo de Modelos en las Organizaciones

Modelo es una representación de cosas o hechos reales en la cual a ex profeso se ignoran algunos detalles o se reproducen en forma destacada algunas características, pudiendo considerarse como un esquema simplificado de la realidad.

Por tanto, modelo es una imagen que trata de representar y traducir, de acuerdo a la estructura de pensamiento del observador, en forma literaria bien de un modo más riguroso y matemático, todos los vínculos que existen entre las funciones de una misma organización y el conjunto de restricciones, tanto internas como del entorno, que se le imponen ya sea a causa de su estructura organizativa, su finalidad, su forma legal, etc.

Un modelo es, necesariamente, una construcción simplificada de la realidad, pero su formulación permite hacer predicciones sobre su comportamiento futuro, conocer las alternativas que se le ofrecen y determinar aquellas que le asegurarán un determinado camino critico. En consecuencia, fundar las decisiones sobre resultados objetivos y limitar o más exactamente acotar el rango de opciones de soluciones, de acuerdo con las posibilidades (en los planos tecnológico, humano y financiero) de la organización.

El empleo de distintos modelos debe conducir a la integración de la organización, si bien hay que reconocer que la integración total es un fin en desarrollo constante que no se agota, es importante una progresiva integración parcial.

La sociedad, la organización y los resultados quedan enmarcados dentro de un entorno que no solamente fija límites reales o geográficos, sino también establece algunas limitaciones.

La Organización Como un Sistema

En tal sentido una organización es un sistema complejo e integral, de tipo intencional o finalístico, cultural o creado y como tal intenta dar, constructivamente, respuesta a las demandas cambiantes (manifestadas en forma explícita o implícita) del medio en el cual se inserta.

El documento ISO 9000:2000 define organización como "conjunto de personas e instalaciones con una disposición determinada de responsabilidades, autoridades y relaciones".

Dicho en la forma más breve y general posible, una organización es un grupo de gente coordinada para la obtención de un fin común, finalista.

Establecida la finalidad es necesario conocer la realidad y analizarla, de modo de establecer la secuencia de acciones posteriores. Para ello es necesario comprender qué principios rigen los elementos interactuantes con qué elementos se cuenta y cómo se estructuran dichos elementos.

El secreto de cualquier organización es, pues, actuar y prever las acciones futuras, entendiendo que el sistema de gestión integrado se va consolidando a medida que se avanza en su implantación

Estructura de los Sistemas De Gestión

El documento ISO 9000:2000 define sistema de gestión como "sistema para establecer la política y los objetivos y para el logro de dichos objetivos"
Por ello los sistemas de gestión, sea en forma individual o integrada, deben estructurarse y adaptarse al tipo y las características de cada organización, tomando en consideración particularmente los elementos que sean apropiados para su estructuración.

Para ello se debe definir claramente:

1. la estructura organizativa (incluyendo funciones, responsabilidades, líneas de autoridad y de comunicación),
2. los resultados deseables que se pretende lograr,
3. los procesos que se llevan a cabo para cumplir con la finalidad,
4. los procedimientos mediante los cuales se ejecuta las actividades y las tareas
5. los recursos con los cuales se dispone.

Los sistemas de gestión se aplican en el marco de todas las actividades que se ejecutan en la organización y son validos solo si cada uno de ellos interactúa con los de más armónicamente.

La estructura de los sistemas de gestión debe ser tal que sea factible realizar una coordinación y un control ordenado y permanente sobre la totalidad de las actividades que se realizan.

Principios Comunes

Estos principios son:

1. **La cultura empresarial.** La identificación de una forma de ser de la empresa, que se manifiesta en las formas de actuación ante los problemas y oportunidades de gestión y adaptación a los cambios y requerimientos de orden exterior e interior, que son interiorizados en forma de creencias y talantes colectivos que se trasmiten y se enseñan a los nuevos miembros como una manera de pensar, vivir y actuar.
2. **Organización enfocada a las partes interesadas**, que se convierten en una finalidad básica. Por ello las organizaciones se integran de diversas formas con las partes interesadas y, en consecuencia, deben cumplir con los requisitos de las mismas.
3. **involucramiento de la gente**. La gente es la esencia de una organización y su involucramiento completo permite el uso de sus competencias y de su experiencia para el beneficio de la organización.
4. **Liderazgo**. Como resultado de lo anterior dentro de la organización la dirección de la misma debe crear las condiciones para hacer que la gente participe activamente en el logro de los objetivos de la organización.
5. **Enfoque basado en eventos**. Todos los resultados deseados se logran más eficientemente cuando los recursos y las actividades de la organización se estructuran, se gestionan y se conducen como eventos. Que en una simplificación se corresponde con lo que llamamos procesos en los sistemas de calidad.
6. **Aplicación de la concepción de sistemas a la gestión**. Consiste en la identificación la comprensión y la gestión de una red de eventos interrelacionados para maximizar la eficacia y la eficiencia de la organización.
7. **Mejora continua**. El mejoramiento continuo de su desempeño global es un objetivo permanente de todas las organizaciones.

8. **Enfoque basado en los hechos para la toma de decisiones**. Las decisiones y las acciones debelan basarse en el análisis de los resultados, de los datos para lograr una optimización de la información que permite tomar decisiones con el menor nivel de incertidumbre.
9. **Relaciones mutuamente beneficiosas con los asociados**. Las relaciones muy beneficiosas con los asociados debelan establecerse para resaltar la ventaja competitiva de todas las partes interesadas.

Operatividad de los Sistemas de Gestión

Los sistemas de gestión adaptados al tipo particular de organización, deben operar de tal manera que se dé la confianza apropiada que:

a) sean bien comprendidos por la totalidad de los protagonista,
b) operen en forma eficaz,
c) los resultados satisfacen las expectativas de las partes interesadas,
d) se enfatiza las acciones preventivas ante cualquier clase de problemas.

Relación Organización Partes Interesadas

Los sistemas de gestión poseen dos aspectos interrelacionados:

a) Los intereses y necesidades de la organización. Para la organización existe una necesidad de alcanzar y mantener los resultados deseados a un costo óptimo, eficiencia. Este logro se relaciona con una utilización planificada y subsecuentemente eficiente de sus recursos.
b) Las expectativas de las partes interesadas. Para las partes interesadas existe una necesidad de confiar en la capacidad de la organización tanto para brindar como para mantener los resultados deseados.

Cualquier sistema de gestión de una organización está diseñado esencialmente para satisfacer las necesidades internas de gestión de la propia organización. Por tanto, es más amplío que lo fijado por los requisitos de las partes interesadas vinculadas con la organización.

Por lo tanto, los sistemas de gestión están influidos:

a. por los objetivos de la organización,
b. por los, procesos que realiza,
c. por la metodología que emplea para la ejecución de los procesos,
d. por los resultados que se espera,
i. por las relaciones que mantiene con todas las partes interesadas,
e. por la influencia que tiene el medio sicosocial y el físico sobre sus actividades.

Por consiguiente, un sistema integrado de gestión varía de una organización a otra. Por ello en el sistema integrado de gestión es necesario identificar todas las acciones que deben ejecutarse, asignar responsabilidades en forma clara y establecer las interrelaciones de cooperación entre sectores. De este modo se favorece la creación de mecanismos para integrar todas las funciones de la organización a la finalidad establecida.

La Gestión por Procesos

Un proceso es la secuencia de actividades orientadas a generar un valor añadido sobre una entrada, consumiendo unos recursos para obtener un resultado conforme a los requerimientos del cliente (interno o externo). La gestión por procesos se centra en la identificación, control y mejora de estos procesos, que son los que realmente añaden valor al cliente.

La estructura de organización más extendida en las empresas y en la nuestra es la organización funcional, por departamentos, con varios niveles jerárquicos. Esta estructura surge fruto de la generalización de la división del trabajo, para coordinar los puestos de trabajo, cada uno especializado en una tarea.

En un entorno con demanda predecible y creciente este tipo de estructura funciona relativamente bien. Pero en un entorno turbulento y que cambia rápidamente la burocracia de control de tareas se convierte en un estorbo, retrasando la reacción ante los cambios y aumentando el coste del producto.

El cliente no está interesado en nuestro sistema burocrático interno de control; lo que busca y lo que valora (y por lo que paga) es el producto o servicio, con determinadas características (calidad, plazo, prestaciones, etc.).

La gestión por procesos contrariamente se centra en la administración del conjunto de actividades enlazadas que generan el producto o servicio, para aislar y tratar por separado aquellas operaciones que no añaden valor para el cliente.

La instrumentación de la gestión por procesos debe:

- Analizar las ineficiencias de la organización funcional para mejorar la competitividad de la Empresa.
- Identificar los procesos que proporcionan una ventaja competitiva y los relaciona con el valor que percibe el cliente.
- Establecer un sistema de control para reducir la variabilidad de resultados.
- Establecer indicadores de funcionamiento y objetivos para dirigir la mejora de los procesos, según el ciclo PDCA de Deming (Planificar, Hacer, Comprobar y Actuar).

La orientación a la gestión por procesos supone un cambio de actitud y mentalidad importante. En lugar de pensar cómo hacer mejor lo que hacemos,

debe reflexionarse por qué y para quién lo hacemos Implica una evolución hacia el trabajo en equipos orientados a los procesos integrados, con mayor grado de autonomía.

Estructura del Sistema de Gestión Integrado

La teoría organizacional moderna define al análisis de sistemas como la manera más adecuada de estudiar las organizaciones, utilizando como herramientas para dicho estudio a una base analítica conceptual caracterizado por la confianza en la observación de los hechos y la naturaleza sintetizadora e integradora.

A su vez, tal como se ha dicho, toda organización está compuesta por varios subsistemas interdependientes, formulados o no, que se asocian entre sí en un único suprasistema. Pero para ello la organización debe seleccionar un estilo de gestión que le sea útil, para llevar adelante todos los subsistemas que la constituyen. De este modo si bien existen estándares, reglas y demás cada organización es peculiar en su instrumentación, implantación y desarrollo por lo que en última instancia no existen sistemas sino organizaciones.

Algunos de los sistemas pueden ser considerados como cerrados en cuanto tienen escasa relación con el medio en el cual asientan o con el suprasistema, lo que puede ser una aproximación útil para la simulación. Otros sistemas pueden ser considerados como abiertos, en cuanto son modificables fácilmente de acuerdo con cambios que ocurren en el medio o en el suprasistema. Pero en última instancia básicamente existe un grado de intercambio mayor o menor de materia, energía, etc., con el medio que siempre debemos considerar.

La teoría de sistemas es una herramienta que ha permitido la integración de los conocimientos provenientes de diversas áreas para facilitar la comprensión de fenómenos que presentan un alto grado de complejidad. Dentro de las que se pueden distinguir varías categorías o niveles jerárquicos de sistemas como:

1. El nivel de la organización en el cual se incluye sistemas estáticos que tienen establecidos ciertos marcos de referencia.
2. El nivel de las funciones principales en el cual se incluye sistemas dinámicos que tienen objetivos generales definidos.
3. El nivel de las actividades en el cual se incluye sistemas dinámicos que tienen objetivos específicos claramente establecidos.
4. El nivel de las tareas en el cual se incluye sistemas dinámicos que tienen objetivos específicos fácilmente mensurables.
5. El nivel de la sociedad, por ejemplo la comunidad en la cual se incluye sistemas dinámicos que tienen expectativas diversas.
6. El nivel de los individuos que tienen conciencia y habilidades tanto para ejecutar acciones como para tomar decisiones.

Paralelamente, la estructura de cualquier sistema debe ser tal que sea factible realizar un control ordenado y permanente sobre la totalidad de las actividades que afectan los resultados así como medir la eficacia del desempeño del mismo.

Dentro de la gestión general de cualquier organización, se debe establecer claramente la estructura de cada uno de los sistemas de gestión particulares y subsecuentemente del sistema integrado. Esto incluye definir claramente la estructura organizativa, como ser procesos a llevar a cabo, procedimientos mediante los cuales se ejecuta las actividades y las tareas, así como establecer los recursos de los cuales se dispone.

Las diversas partes del sistema de gestión de una organización deben integrarse en un sistema de gestión único, coherente y unificado que utilice elementos comunes. Esto facilita la planificación, la asignación de recursos, el establecimiento de objetivos complementarios y la evaluación de la eficacia.

La integración es una forma eficaz de ahorrar costos, mejorar la comunicación dentro de la misma empresa y obtener una mayor integración en la estrategia de la empresa. [1]

Gráfico 30: Elementos de un Sistema de Seguridad Corporativa

Elementos del Sistema

Existe un paralelismo total entre los requerimientos de ambas normas (ISO 14001 y OHSAS 18001). Los mismos se resumen en: Política Corporativa, Planificación, Implementaron y Operación, Verificación y Acciones Correctivas y, por último, Revisión Gerencial.

[1] Rubio Romero, Juan Carlos. López Toro, Alberto. Negro Mellado José. Los Sistemas Integrados de Gestión de la Calidad, el Medio Ambiente y la Prevención de Riesgos Laborales. Conexiones, ventajas e inconvenientes, proceso, estructura y normas para su diseño e implantación. Universidad de Málaga. E.T.S.I, España.

Documentación

El Sistema de Gestión Integrado se apoya en documentación escrita, cuya función es guiar y controlar todas las acciones para el logro de los objetivos y su propósito principal es asegurar que todo el personal tanto el de Organización como de los contratistas, está utilizando los mismos procedimientos e instrucciones de trabajo en una misma forma consistente.

Los principales documentos son:

- El manual de gestión integrado, que describe en forma genérica la estructura del sistema de gestión ambiental y de seguridad y hace referencia a los documentos del mismo.
- Los manuales de procedimientos especifican la forma de realizar las actividades vinculadas al sistema, las distintas responsabilidades, los mecanismos de control y los registros obtenidos.
- Los procedimientos de gestión son los que regulan el funcionamiento y estructura del sistema; los operativos controlan las actividades y procesos propios del área y se vinculan con los efectos ambientales significativos.
- El plan de contingencia debe describir todos los mecanismos a seguir ante situaciones de emergencias.
- Los registros fundamentales para el sistema son: Registro de normas aplicables, el registro de **aspectos/impactos físicos** y el registro de **aspectos/impactos de salud** (peligros/riesgos).

Implementación y Operación.

Finalizada la fase de diseño, se requiere poner en práctica una serie de elementos exigidos por las Normas. Estos se explican a continuación.

Estructura y Responsabilidad

El Sistema no podrá entrar en funcionamiento a menos que se establezca una estructura organizativa que permita la adecuada movilidad requerida. Existen distintas variantes en nuestro caso hemos optado por armar un equipo que lidere todas las decisiones. Este equipo lo denominamos "Centro de Coordinación y Control" (CCC), al cual están vinculados los principales líderes de la Operación, comenzando por el Gerente mismo. La implantación y mantenimiento del sistema es responsabilidad del CCC y alcanza a todo el personal que cumple sus funciones en el lugar. Las gerencias operativas proveen a todo el personal de los medios que garanticen la formación y el adiestramiento adecuado para las tareas que cada uno desempeña. Las soluciones podrían ser otras, pero esta vía ha permitido un rápido desarrollo del Sistema y el cumplimiento de sus objetivos.

Capacitación, concientización y comunicación.

La capacitación es un componente esencial y crítico del Sistema, señalamos los aspectos o recomendaciones más importantes:

- Hacer énfasis en los elementos constituyentes del Sistema. No se trata solamente en capacitar sobre destrezas operativas requeridas para minimización de impactos y riesgos, sino principalmente adiestrar sobre aspectos que fortalezcan a la Organización en el conocimiento del Sistema de Gestión en sí mismo. Por ejemplo, habrá que difundir la Política de la Empresa a través de diversos medios, pero también mediante la Capacitación. También habrá que adiestrar al personal sobre las Normas y Leyes Aplicables más relevantes para las Operaciones; así mismo, la capacitación sobre Planes de Contingencia, Procedimientos Operativos, entendimiento sobre las Normas a certificar (ISO14001 y OHSAS 18001), entendimiento sobre la esencia de cada elemento del Sistema y su conexión, etc.

- Debe ser organizada y planificada entre el Departamento de Ambiente y Seguridad Industrial, Recursos Humanos y los Sectores Operativos involucrados.
- No se trata de un Programa de Adiestramiento pasivo. La gran mayoría de los talleres y cursos deben ser ejecutados con esfuerzo propio, particularmente por parte de los sectores operativos, sentido de pertenencia del Sistema a nivel de toda la estructura organizativa.
- Diseñe una buena estrategia de comunicación. Debe hacer comprender a la Organización la importancia del adiestramiento a recibir o recibido y que también sea diseñada para reforzar los conocimientos aprendidos. Mediante una adecuada capacitación y comunicación continua se logra avanzar en las diversas etapas conducentes a alcanzar un avanzado nivel de conciencia sobre sus responsabilidades y papel a desempeñar para lograr la buscada minimización de impactos y riesgos. En toda organización en donde se comience a introducir los conceptos relacionados con el Sistema, el personal suele iniciarse, en mayor o menor grado, con un muy bajo nivel de concientización que podría ser descrito como un personal tanto inconsciente de sus riesgos y potencialidad a ocasionar impactos, como también incompetente para lograr el control o mitigación de los mismos. Con el tiempo e intensificación la capacitación, esa misma persona, comienza a comprender su papel, funciones y efectos positivos del Sistema para contribuir a mitigar impactos y riesgos; es decir, pasa a ser consciente de los mismos, pero quizás mantiene cierto grado de incompetencia para decidir con precisión lo que debe hacer. A través de estas etapas de madurez de los individuos respecto al Sistema, se entra en una tercera etapa que podríamos denominar de "consciente y competente"; es decir, ahora el individuo no solo está consciente de sus riesgos sino que conoce bien lo que debe hacer. Sin embargo, la etapa más deseada en ese proceso de maduración, se alcanza cuando la Organización logra un alto nivel de competencia para decidir como minimizar impactos y riesgos, y cada uno de sus individuos logra internalizar tan profundamente sus funciones que podrían considerarse como "actos reflejos"

que no necesariamente requieran de alguna reflexión o conciencia de los riesgos de la operación.

Documentación y su control.

La Auditoría de Certificación impondrá al grupo auditor tener sus hallazgos de manera bien fundamentada, porque cualquier demostración relativa a los elementos del Sistema tiene que estar bien documentada. La documentación perteneciente al Sistema debe estar organizada y controlada, bien sea con sus soportes en papel o mediante archivos electrónicos. Así como, buena parte del éxito en obtener la Certificación, dependerá del diseño de adecuados controles de documentación, que sean lo suficientemente robustos y organizados. Como cada Organización y Sistema de Gestión poseen sus particularidades propias no existe un modelo único. La Organización lo diseña, lo adopta y lo modifica de acuerdo a la evolución del mismo y a sus propias características.

Control Operativo.

No existe una única manera en que una Organización deba diseñar sus métodos de Control Operativo. Todo dependerá de la naturaleza de las operaciones en cuestión y la manera en que se adecuen los operarios para mantener el mejor seguimiento posible de lo que hacen. A la hora de una Auditoria no deben plasmarse por escrito nada que no refleje la manera en que se ejecutan las cosas.

El resto es materia de diseño y formalizar un modelo confiable de control operativo.

La redacción de cada uno de estos procedimientos debe seguir rigurosamente los formatos ISO y tratar, en lo posible, de no caer en detalles excesivos, pero sí ser amplios sobre la ejecución de las actividades, destacando las medidas de mitigación de impactos y riesgos.

Planes de Contingencia y Respuesta ante Emergencias.

Ambos sistemas integrados apuntan en su esencia en el sentido de la prevención y la atenuación y la remediación es el remedio de lo no posible. El propio sentido de la mejora continua marca la orientación del planificador. Sin embargo, desde la incertidumbre determinista o no la Organización debe estar preparada estructuralmente, para dar respuesta a aquellas situaciones que se salen del los márgenes previstos de control. El concepto de Tecnologías de Final de Tuberías de la gestión ambiental es permutable o equivalente al método de interposición de "barreras" en Salud y Seguridad. Este aspecto es uno de los más importantes de la etapa de implantación y operación del Sistema de Gestión, que debe ser capas de actuar organizadamente y con rapidez ante cualquier eventualidad de accidentes bien sean de repercusión ambiental, sobre los bienes materiales de la empresa, su personal o terceros. Una vez ocurrido el evento, entran en acción todas las medidas contemplada en los Planes de Contingencia y Respuestas ante Emergencias pertenecientes al Sistema de Gestión. Su papel fundamental está en detener la propagación y magnificación del evento, hasta llevarlo a una condición de control total.

Los Planes de muchas empresas del mundo son coincidentes y suelen incluir aspectos muy similares, siguen en general diseños puestos en práctica y aceptados a nivel internacional. Pero es necesario mantener una gran claridad en lo que habrá de ser el producto final, ya que aun siendo expertos en el tema, es necesario conocer a fondo el funcionamiento del Sistema de Gestión e, inclusive, la operación misma.

Verificación y Acciones Correctivas.

Cuando el Sistema de Gestión Integrado este en plena operación, se requieren acciones de verificación del cumplimiento de los acuerdos, pautas y elementos

pertenecientes al Sistema. Disponemos de tres herramientas de acuerdo a las normas:

1) Mediciones y seguimiento.
2) Los reportes y registros de Accidentes/incidentes y de no conformidades/acciones correctivas.
3) Las Auditorías.

Mediciones y seguimiento.

Se refiere a todas aquellas acciones que se hacen en la operación y que permiten cubrir los requisitos legales en cuanto a medición de parámetros exigidos por las normas y regulaciones o bien, garantizar que los equipos y procesos asociados a la operación se encuentren a niveles de óptimo desempeño. El centro integrador es el proceso y es quien debe focalizar la acción. El grupo auditor insiste en este aspecto de la Norma, porque al estar ligado a la integridad de la operación misma, posee un fuerte impacto en la verificación del buen funcionamiento del Sistema de Gestión, según lo indicado por **Paco Vila (Internet: 2011)**.

Desarrollo del Sistema de Seguridad

Pasos Previos

Paso 1: Definición de los Riesgos más Relevantes

Los esfuerzos de Prevención de Pérdidas y Seguridad deben centrarse en los riesgos más relevantes

Paso 2: Objetivos de Protección.

Dentro de cada empresa existen instalaciones, procesos e información que son parte de lo que se llama el Core Bussines (Corazón del Negocio). Se adiciona a ello, y por eso no es menos importante, al personal de la empresa.

Paso 3: Evaluación de la tecnología y equipamiento de seguridad y prevención de pérdidas

El nivel de tecnología y equipamiento de seguridad dependen de cuán complejos son nuestros objetivos de protección.

Paso 4: Evaluación de las Políticas, Planes y Normas de seguridad y prevención de pérdidas.

Si una empresa no tiene Políticas, Normas y Procedimientos de Prevención de Pérdidas y Seguridad correctamente establecidos y difundidos, es porque no es consciente de que esta es una herramienta que le ayuda a lograr objetivos de negocio…y por tanto, está en desventaja competitiva.

Paso 5: Evaluación de las Auditorias y Controles de Seguridad.

Lo que no se controla no se gestiona y se pierde en el tiempo… De nada sirve tener recursos de seguridad si no se verifica permanentemente y/o periódicamente que todo está marchando de acuerdo a las expectativas y orientado hacia lo que el negocio exige.

Paso 6: Evaluación de la Cultura y Capacitaciones respecto a temas de seguridad y prevención de pérdidas.

Lo óptimo de la Seguridad en una empresa es llegar a un estado de interdependencia, vale decir, donde todo trabajador es consciente que su seguridad

depende de los demás y viceversa. Para llegar a este estado se necesita de la permanente disposición y liderazgo de las gerencias, jefes de línea y supervisores, y también de incorporar los temas de seguridad dentro de los planes de capacitación anuales.

Paso 7: Información, Inteligencia y Comunicaciones

Todos los recursos asignados a la seguridad de la empresa deben generar información relevante y suficiente para la toma de decisiones. La creación y uso de Base de Datos resulta de vital importancia para generar estadísticas que permitan alertar y actuar a tiempo. Por tanto, desde el punto de vista gerencial es necesario resolver las siguientes inquietudes:

Elementos

- Normatividad corporativa en la materia.
- Seguridad del personal y seguridad física.
- Seguridad de la información.
- Seguridad logística.
- Metodologías para la gestión corporativa de seguridad.
- Prevención y detección de delitos.
- Manejo de riesgos.
- Seguridad e higiene industrial.
- Investigaciones.
- Planes de continuidad del negocio.
- Procedimientos para evitar fraudes.
- Plan de manejo de crisis.
- Capacitación, en seguridad, del personal.

Al igual que un proceso administrativo, un sistema de seguridad tiene algunos pasos básicos lógicos:

- **Defina objetivos.** Cuál es la finalidad, qué tipo de amenazas y riesgos quiere prevenir, con base en sus necesidades actuales y su presupuesto.
- **Mida y evalúe los sistemas actuales.** Si ya existen sistemas electrónicos o procesos de seguridad implementados, evalúe si son funcionales y efectivos. Normalmente, las empresas ya cuentan con la infraestructura básica necesaria, pero ésta es mal utilizada. No siempre es necesario invertir en nuevos equipos y tecnologías. Se debe aprovechar lo que la empresa ya tiene, de ser posible. Si la solución que propone para eliminar una pérdida o evitar una amenaza, tiene un costo mayor a la misma perdida o efecto de la amenaza, probablemente una buena decisión sería asumir el riesgo y absorber esa pérdida, dado que tendrá un costo menor para la empresa.
- **Analice para eliminar brechas.** Cuáles son las áreas de oportunidad con base en los objetivos
- **Mejore, sea creativo.** En este proceso puede auxiliarse de expertos en diversos temas relacionados con la seguridad, como pueden ser seguridad electrónica, informática, capacitación en seguridad. Muchas veces, las recomendaciones para elevar el nivel de seguridad de una empresa son de bajo costo e implican aplicar creatividad, capacitación y nuevos procedimientos de control.
- **Controle - institucionalice el sistema mejorado.** tendrán que contar con controles e indicadores de gestión que permitan medir resultados, evaluar su efectividad para poder implementar procesos de mejora continua. Además, deberá formalizar y generalizar su aplicación a lo largo y ancho de toda la organización, con el apoyo de la alta dirección. Dentro de los procesos de inducción de nuevos empleados, deberá incluirse el tema de la seguridad corporativa. El esfuerzo de un sistema de seguridad de seguridad no debe quedar como un documento "oscuro y desconocido" en una carpeta más, almacenada en un archivero en la oficina del responsable de seguridad.

Manejo de Crisis

El manejo de crisis es un proceso por medio del cual una organización trata con algún evento que amenaza con hacer daño a la organización, a sus accionistas o al público en general. Tres elementos son comunes en todas las definiciones de Crisis:

- Una amenaza a la organización.
- Un elemento sorpresa.
- Un periodo de tiempo corto para tomar decisiones.

Es, especialmente por este último elemento, por lo cual se debe considerar el Plan de Manejo de Crisis dentro del Plan Corporativo de la organización desde un principio.

Existen seis características que alinean a la seguridad con el negocio:

- El principal papel del responsable de seguridad es convencer a sus colegas, a lo largo de la organización, a actuar con una conciencia de seguridad en sus acciones y decisiones diarias; no a tratar de hacer seguridad para o por la empresa.
- El departamento de seguridad debe estar en el negocio del cambio, más que en la imposición, y trabaja a lo largo de redes sociales de influencia confiables.
- Seguridad está para ayudar a la empresa a asumir riesgos, más que para prevenirlos y, por lo tanto, debe estar dentro del equipo al frente del nuevo desarrollo del negocio.
- Seguridad responde, frecuentemente, a nuevos retos y preocupaciones del negocio y, como tal, el portafolio de responsabilidades y su importancia relativa cambiará con el tiempo. Los departamentos de seguridad nunca deberán permanecer estáticos. En muchas empresas, hoy en día, su rol está

más involucrado con la capacidad de recuperación que con la seguridad "tradicional".

- Seguridad es una actividad tanto estratégica como operativa, y los departamentos deben distinguir entre estas dos funciones.
- El poder y la legitimidad del departamento no proviene solamente de su experiencia, sino de su perspicacia del negocio, de habilidades personales, de su capacidad de administración y comunicación efectiva.

Aspectos a implementarse

Publicación de Información

- Ante cualquier duda sobre el tratamiento de información, consultar al Responsable Funcional de Aplicación o al Responsable de Seguridad.
- Distinguir cuando se hace un uso acorde a la finalidad declarada de los datos de carácter personal.
- Los datos de carácter personal son propiedad de su titular, no de quien los custodia.
- El Responsable del Fichero debe autorizar cualquier uso extraordinario de los datos.

Acceso a los Sistemas de Información

- Existe un procedimiento para solicitar acceso a los Sistemas de Información.
- Éste debe constar como anexo del Documento de Seguridad y debe estar actualizado por el centro.
- El Responsable Funcional de Aplicación debe ser la figura a la que el usuario/profesional consulte la mayoría de sus dudas respecto de los datos de carácter personal.

- Las credenciales de un usuario relacionan a éste con sus acciones en los Sistemas de Información, Responsabilidades.

Análisis de la Infraestructura por aplicación crítica.

Seguridad Física.

- Monitoreo ambiental
- Control de acceso
- Desastres naturales
- Control de incendios
- Inundaciones

Seguridad en las conexiones a Internet.

- Políticas en el Firewall
- VPN
- Detección de intrusos

Seguridad en la infraestructura de comunicaciones.

- Routers
- Switches
- Firewall
- Hubs
- RAS

Seguridad en Sistema Operacionales(Unix, Windows)

Correo Electrónico

Seguridad en las aplicaciones

Auditoría de seguridad de sistemas de información

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales generalmente por Ingenieros o Ingenieros Técnicos en Informática para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Fases de una auditoría

Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas.

Tipos de auditoría

Los servicios de auditoría pueden ser de distinta índole:

- Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.
- Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de los

softwares y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Estándares de Auditoría Informática y de Seguridad

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas practicas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar podemos encontrar el standard ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

Normas de Seguridad Corporativa

Protección de la Información

La protección de la información es, hoy, vital para la supervivencia de cualquier organización. Esto no es un secreto. Sin embargo, descuidamos esta faceta de nuestra seguridad, regalando oportunidades, a cualquiera que quiera saber algo de nosotros. Estamos acostumbrados a tener alarmas, cerraduras, etc. para proteger nuestros bienes, pero descuidamos lamentablemente, la protección de algo intangible, pero mas importante, nuestra intimidad. En estas breves hojas, lo único que pretendo es alertarle sobre algunos riesgos, y darle algunas soluciones sencillas. Le ruego que las lea con detenimiento, y las aplique, ya que son de práctica general en aquellas Organizaciones que están concienciados sobre estos temas (y que suelen funcionar mejor que el resto)

Antes de empezar

No es mi intención el darle una información suficiente para que usted pueda transformarse en un técnico, sino darle algunos conceptos, para lo que se conoce como "Protección de la Información", que es algo más amplio que la detección de escuchas, sea algo más que un nombre raro, y usted y su Organización puedan vivir un poco más seguros.

Lo que pretendo es dar la información imprescindible a cualquier responsable de Protección, para que sepa lo que debe hacer, pueda leer otros textos ampliatorios, y obtenga el máximo de los servicios que le puedo prestar.

Lo que sí es importante, es que todas aquellas medidas preventivas que se relacionan, las conozca, y sea capaz de obligar a ponerlas en práctica a su Organización, como manera más sencilla y barata de evitar las escuchas. Y evitar la "cara de tonto", que se le pone a la gente, cuando descubre que hace meses que le están escuchando sin darse cuenta.

Es importante destacar que de lo que se trata es de proteger un "intangible", y normalmente será lo más valioso de una empresa, es decir, el conocimiento, o como normalmente se conoce: la información.

Pasó la época en la que el principal papel de la Seguridad era la protección de unas instalaciones, de unas materias primas o elaboradas, de unos medios de producción. Hoy, en plena economía de la "tercera ola", el principal capital de una organización son las personas y sus conocimientos, y los conocimientos de producción, ventas, mercado, etc. que la Empresa posee. Hoy es mucho más ruinoso para una fábrica la pérdida del "backup", que la destrucción física de las instalaciones de producción. Y eso que es del sector secundario. En el terciario la pérdida es absoluta. Hoy la única diferencia entre una empresa de éxito y las

demás, es que "saben" más, y lo aplican con mejores métodos. Y como es lógico, las demás intentaran saberlo, y por cualquier medio.

Importancia de la protección de la información

La relativa tranquilidad existente en España en materia de espionaje industrial y comercial lleva a que sistemáticamente se diagnostique como paranoico a todo aquel que manifieste una mínima preocupación por la seguridad en el tratamiento de la información.

No obstante, lo cierto es que en la empresa actual el valor más importante radica en la información. Han pasado ya los tiempos en que los elementos productivos eran la base efectiva del negocio y hoy, más importante que la máquina es la información que permite saber qué, cómo y cuándo hacer algo. Sin consideración a la bondad o maldad de dicha situación, la sociedad americana viene a ser el paradigma de la asignación de recursos bajo criterios de imprescindibilidad.

Desde el momento en que la industria americana destina importantes sumas de dinero a cuidar su seguridad, resulta evidente que por algo lo hará. Y ese algo es que muchas empresas han sufrido el daño que causa una fuga incontrolada de información.

El principal problema que plantea esta cuestión es que todos estamos de acuerdo en que la falta de control sobre la información es un riesgo latente, pero muchos ven difícil la materialización del mismo en un momento dado. Que en un determinado momento no se den las circunstancias propicias para temer un intento de acceso a nuestra información interna no significa que éste no vaya a producirse, ello independientemente de que el número de posibles amenazas es, generalmente, desconocido por nosotros mismos.

Es evidente que un competidor puede estar interesado en nuestros secretos. Pero no es el único que puede estarlo. Un trabajador resentido, un periodista ávido de escándalos, un grupo de investigación estatal, un miembro de nuestro propio equipo de trabajo, etc., pueden estar interesados en determinada información, sea para fines lícitos o ilícitos. Podemos tener una relativa tranquilidad de que nuestros competidores no iniciarán una guerra ni utilizarán tácticas ilegales para apoderarse de nuestros secretos. Pero no podemos presumir lo mismo de cuantas personas crean que podrán obtener un beneficio por el conocimiento de nuestra información. Sencillamente porque no podemos saber quién puede creer eso.

Incluso respecto de compañías competidoras en un mercado tranquilo tal presunción es temeraria y la historia reciente lo demuestra. El hecho de que una persona no considere determinadas prácticas como propias del mercado no significa que otra, carente de tales escrúpulos, no las utilice, ahora o en el futuro. Y nadie puede determinar la fecha, exacta o aproximada, de ese futuro.

La moderna tecnología permite llevar a cabo sistemas de espionaje con un ámbito extraordinario, de forma imperceptible y con total impunidad. Baste como ejemplo señalar que, hoy en día, por menos de 15 millones de pesetas se puede adquirir en el mercado un equipo capaz de monitorizar todas las conversaciones mantenidas a través de un teléfono móvil GSM, independientemente del lugar donde esté su usuario. O un dispositivo para intervenir teléfonos (de la mejor tecnología), no llega a las 100.000 Si comparamos estas cifras con el presupuesto invertido por la modernas compañías en estudios de mercado veremos lo irrisorio de su importe. ¿De verdad alguien está convencido de que nadie es capaz de invertir estas cantidades para conocer nuestros secretos?

Pero, además, el riesgo no está, ni exclusiva ni principalmente, en el acceso de firmas competidoras a la información interna de una compañía. Incluso en el seno de la propia empresa, un acceso incontrolado a la información es fuente de

conflictos imprevisibles y, en la mayoría de los casos, de sospechas mutuas que enturbian el clima de trabajo.

Nadie puede valorar el efecto que producirá en un tercero una determinada información. Por ello, toda la información debe ser objeto de protección frente a fugas incontroladas. Incluso la inútil.

Veamos, si no, un ejemplo real. Una compañía prevé un estancamiento y posterior recesión del mercado. El Director Financiero establece un plan de austeridad de gastos, materializado en un presupuesto restrictivo. La situación no es agradable y, como entretenimiento, introduce en el mismo programa de simulación una fantasía: mercado en expansión y aumento de ventas. Todos los directivos agradecen la distensión que supone romper la decepción que el verdadero informe ha supuesto. Finalizada la reunión, el Director Financiero guarda bajo llave el informe real. Y deja sobre su mesa la simulación inútil. ¿Qué problema hay, si es información falsa? El resultado de todo ello es un pobre Director de Recursos Humanos casi desquiciado tras una semana de negociación de la renovación del convenio laboral de la empresa por la incomprensible necedad del Comité de Empresa, obstinado en negar un hecho tan evidente como el estancamiento del mercado y la prevista disminución de las ventas. Una copia del informe falso había llegado a manos de los trabajadores.

Otro ejemplo real. Un directivo nota repentinamente un cambio en la actitud y disposición al trabajo de uno de sus colaboradores directos. Sin una explicación deducible, baja su rendimiento, su carácter es pasivo y su trato frío y distante. Lo que ocurrió, y el directivo desconocía, es que dejó en un cajón de su mesa su propuesta de aumentos salariales para el personal del departamento y tal trabajador pudo comparar su situación con la de otros.

La información personal debe ser también objeto de especial protección y reserva y ser facilitada sólo respecto de datos imprescindibles y, al margen de otros

directivos, a un único colaborador de especial confianza. Datos como el domicilio y teléfono particulares, segundas residencias, tenencia y localización de bienes de recreo, etc., son datos intranscendentes en situaciones de normalidad. No obstante, con ocasión de despidos disciplinarios, expedientes de regulación de empleo o huelgas, un piquete informativo en poder de dicha información puede ser una auténtica pesadilla. Esta disponibilidad incontrolada de información personal por parte de terceros es especialmente peligrosa cuando versa sobre aspectos más íntimos.

Las notas anteriores pretenden ser únicamente una llamada de atención sobre los riesgos que supone la falta de control sobre la información y destruir la idea preconcebida de que sólo determinada información es importante.

Ningún sistema de seguridad puede garantizar un cien por cien de eficacia, ni tampoco se puede llevar la seguridad hasta extremos de paranoia que imposibiliten el normal funcionamiento de la empresa.

Pero sí es posible establecer unas normas mínimas de seguridad en el tratamiento de la información. El objetivo es limitar las fugas incontroladas y permitir la detección de éstas en caso de que se produzcan, a través de una serie de precauciones.

Recuerde, no obstante, que ningún plan de seguridad es infalible. Una cerradura se puede forzar, una clave descifrar y un teléfono siempre se podrá pinchar. Si verifica que no hay dispositivos de escucha en una sala eso sólo significa que en ese momento y lugar no los hay, pero no que no los haya habido ni que no los haya mañana. Si descubre un equipo espía, sólo sabrá que le han espiado, pero no desde cuándo.

La virtud de todas las medidas que se expondrán en este documento no es hacer imposible las intromisiones. Su virtud es que las hace francamente difíciles y, si

tenemos suerte, más difíciles que respecto de firmas competidoras. Sea consciente, no obstante, de este límite.

Lugar de trabajo

El centro en el cual confluye más de 90% de la información que manejamos es nuestro propio lugar de trabajo y, por ello, merece ocuparse de él en primer lugar.

Las principales normas a tener presente en este apartado son las siguientes:

- La sala debe reunir unos requisitos mínimos de aislamiento acústico que impidan la escucha desde el exterior de conversaciones mantenidas en el interior. Esto incluye acristalamiento doble y paneles o paredes aisladas. En caso de que la sala linde con finca vecina, debe preverse una cámara de aire entre el panel interior y la pared. El panel interior debe tener aislante acústico y ser practicable para la inspección de la cámara. Debe disponer de cortinas y cerradura interior de las ventanas, en el caso de que éstas sean practicables.
- Asegúrese, a través de personal de mantenimiento, de que no hay cableado inútil en paredes y falso techo. Puede ser fácilmente utilizado como portador de señal. En caso de instalaciones de reserva (habitual en modernas instalaciones de redes de voz y de datos), verifique que los conductos de canalización son seguros.
- Tenga siempre cerradas las cortinas.
- No utilice ni interfonos ni teléfonos inalámbricos y, en caso de que el uso de los mismos sea imprescindible, adquiéralos de tecnología digital de transmisión.
- Disponga de cerraduras seguras en todas las puertas, armarios y cajones. Si maneja documentos especialmente sensibles, adquiera una caja de seguridad para almacenar los mismos. Dichas llaves deberán estar en su poder y, en caso necesario, en el de su secretaria o colaborador de confianza. En previsión de emergencias, entregue una copia al responsable de seguridad, dentro de un

sobre de seguridad cerrado y con su firma en la unión de la solapa con la bolsa, para su depósito en una caja de seguridad.

- Sólo deben tener acceso a nuestro despacho personas de la propia organización. Las visitas de terceros es conveniente atenderlas en salas especialmente previstas para ello. Además, instruya al personal de limpieza para que revise y adecue la sala inmediatamente después de cada uso. Dichas salas deben carecer de teléfonos enlazados a líneas directas y, en la medida que el sistema lo permita, sólo deben poder realizar llamadas a extensiones interiores (sin perjuicio de que puedan recibir, transferidas, llamadas externas).
- Autorice el acceso a su despacho, en su ausencia, a una única persona de confianza (p.e. su secretaria). En caso de que, en su ausencia, algún colaborador precise de algún documento, ésta será la encargada de entregarlo.
- Al abandonar el despacho, no deje ningún documento accesible. Durante su ausencia, personas sobre las cuales no tiene ningún control accederán al mismo (personal de limpieza, mantenimiento, seguridad, etc.). No presuponga ni la integridad ni la capacidad de estas personas, no todas tendrán su inteligencia y formación para discernir la bondad o maldad de una determinada conducta. Una práctica útil en este aspecto es disponer de un estante en uno de sus armarios, exclusivamente para depositar en el mismo los documentos existentes sobre su mesa en el momento de salir. Instruya a su secretaria o colaborador de confianza a que, antes de salir y en caso de ausencia de usted, revise que no queden papeles accesibles.
- En su ausencia, los armarios y cajones deberán quedar cerrados.
- Disponga de destructora de documentación, de prestaciones adecuadas al volumen de los documentos que maneja. Escoja una que disponga de entrada de objetos al depósito y elimine las papeleras, así estará seguro de que cumple la norma de destruir todo papel desechado. Disponga lo mismo para su secretaria.
- Desconfíe de los regalos. La forma más fácil de introducir un micrófono emisor en su oficina es introduciéndolo en un objeto de regalo. En todo caso,

verifique por personal especializado (a través del responsable de seguridad) su inocuidad. Bajo ningún concepto conecte a la red eléctrica o telefónica equipos que le hayan sido regalados (desconfíe especialmente de un teléfono móvil, se pueden "trucar" de varias maneras).

- En zonas de despachos panelables, no reciba visitas. Es muy fácil que esa persona vea o escuche algo que no debe. Disponga de otro local, donde se recibe, y no se pueda llevar, más que lo que usted le quiera dar.
- Instale una alarma, conectada a Central Receptora, con detectores de humo (no olvide el riesgo del fuego), y mejor con cámara de TV, para que desde la Central sepan lo que está pasando cuando se dispara la alarma.

Proteja la información

Sea cauto en sus conversaciones con colegas en firmas competidoras. Usted nunca podrá valorar de forma segura hasta qué punto una información puede o no ser valiosa para una empresa competidora. Conocer la existencia de un proyecto descartado, aunque puede no parecerlo, tiene una extraordinaria importancia: da una idea de la actividad de una empresa en materia de innovación, afianza la conclusión de que una idea es digna de tenerla presente y estudiarla, permite prever posibles actuaciones futuras, etc. Si, además, comentamos por qué lo hemos descartado, la información (y los beneficios de conocerla) se multiplican.

Y todo sin que seamos conscientes de ello: la mayoría de las veces, las indiscreciones por nuestra parte no son más que respuestas, aparentemente intranscendentes, a indiscreciones ajenas.

Tengamos presente, además, que comunicar determinados detalles o informaciones es la mejor forma de crear confianza en nuestros interlocutores.

Dejar que terceros conozcan estos detalles les permite crear la apariencia de una condición que nunca hemos querido darles.

Uso del teléfono

La comodidad que representa el teléfono hace que por el mismo circule la mayor parte de la información que conocemos. No obstante, es un sistema de comunicación altamente vulnerable: se puede pinchar en todo el recorrido de la línea (tanto interna como externa), el emisor se puede alimentar de la propia línea y la escucha se puede realizar a distancia con total impunidad.
Obviamente, no puede usted prescindir del teléfono, pero sí tomar una serie de precauciones que inutilicen en gran medida todo intento de intromisión.

- Nunca utilice líneas directas al exterior. Aunque su extensión tenga asignado un determinado número entrante, haga programar la centralita para que la asignación de líneas salientes sea aleatoria. De esta forma, para acceder a sus comunicaciones desde el exterior será preciso pinchar todos los enlaces de la empresa.
- En la medida de lo posible, haga instalar líneas RDSI, o similares de transmisión de señal digital. Aunque existen equipos capaces de interceptar dichas líneas, su disponibilidad es mucho menor que los de líneas analógicas (pero el que disponga de tecnología adecuada, podrá hacerle multitud de ataques, imposibles en las líneas analógicas)
- Sea especialmente reservado cuando utilice teléfonos móviles (incluidos los GSM). Es el sistema más vulnerable y que ofrece mayor impunidad. Evite dar nombres o datos cuando hable por el móvil y limite su uso a casos de estricta necesidad. No facilite su número móvil más que a su secretaria de confianza, responsable de seguridad y personal directivo: en caso de necesidad, su secretaria puede transferirle directamente las llamadas urgentes recibidas en su oficina. Active la ocultación del número propio (sólo posible en GSM). Utilice un teléfono o tarjeta independiente para asuntos personales. Debe saber, además, que el GSM, informa al sistema del lugar geográfico en que usted se encuentra, simplemente por el hecho de estar conectado.

- En momentos de especial sensibilidad de los asuntos que deba tratar, adquiera para su teléfono móvil una tarjeta pre-pago, adquirida en efectivo. Posteriormente, desviamos nuestro número habitual al nuevo, y la gente que nos llame, no tendrá que saber el número donde se ha desviado. La tarjeta es el único identificador del equipo y, sin poderla vincular a través de pagos por domiciliación bancaria o tarjeta de crédito, difícilmente será conocida por terceros.

Seguridad informática

En nuestros ordenadores se concentra la práctica totalidad de la información que elaboramos. Además, hoy en día es un medio habitual de comunicación. La utilidad del ordenador para almacenar y procesar información tiene, como contrapartida, la concentración de la misma en un único archivo de escaso tamaño. Antaño, para apropiarse de los secretos de otro había que examinar y sustraer un considerable volumen de documentación. Hoy basta con apropiarse de un objeto que cabe en el bolsillo.

- Utilice un programa de control de acceso y cifrado automático de datos sensibles (SAFE Data BECKER o similares). Los controles por contraseña de los sistemas operativos al uso no cumplen de forma eficaz con esta misión y son altamente vulnerables. Además, no protegen la información frente ataques directos al soporte físico de la misma (generalmente, el disco duro) . Con los portátiles, esto es imprescindible, por lo fácilmente que se pueden "distraer" en cualquier desplazamiento. El cifrado es especialmente importante cuando se trabaja en red, ya que determinados programas, permiten ver todos sus archivos, desde cualquier otro PC conectado a la red (Estos programas están en las revistas especializadas y en Internet, gratuitamente) . O para el caso del correo electrónico, que es muy vulnerable.
- Utilice contraseñas seguras. Palabras, nombres, fechas o secuencias de números son fácil y rápidamente comprobadas a la velocidad actual de

proceso de los equipos. Una contraseña mínimamente segura se compone de un mínimo de 8 caracteres mezclando mayúsculas, minúsculas, números y signos especiales. Y por descontado, créelas usted, no el Dept. de Informática

- Realice siempre copias de seguridad. Si le roban el equipo, o sufre alguna avería, podrá recuperar su trabajo. Almacénelas, eso sí, en lugar suficientemente seguro.
- Active utilidades de cifrado en sus mensajes de correo electrónico (recomiendo el PGP, de uso muy extendido) incluso dentro de la propia red corporativa. Todos los sistemas de correo (internos o externos) están basados en el almacenamiento de los mensajes en un equipo servidor y un operador con autorización suficiente (por clave propia o mediante clave ajena conocida) a los que se podría acceder a los buzones de mensajes sin que usted ni el destinatario lo supieran. No presuponga que el departamento de informática es seguro: probablemente lo es, pero usted no puede saberlo (de todas maneras, piense que el correo electrónico se comporta allí por donde va pasando como un sobre transparente y si alguien quiere, lo puede leer). Utilice direcciones de correo electrónico anónimas, gratuitas y de un solo uso, para los documentos delicados (el servidor de correo de la empresa, para el Dpto. de Informática, es transparente).

Seguridad Corporativa

Todas las normas anteriores serán ineficaces si no son observadas por los miembros de su equipo de trabajo y por el resto de los directivos. Instrúyales sobre la importancia de la seguridad y control en el tratamiento de la información. Distribuya copias de este documento. Mal se pueden tomar medidas de seguridad, cuando se ignora su lógica.

Realice periódicamente "limpiezas", pero especialmente en épocas de crisis. Los "malos" no quieren ser descubiertos, y por lo tanto, es posible que no lo intenten, si saben que se hacen revisiones.

Valore la oportunidad de elaborar una política global de seguridad por profesionales expertos. Esto permitirá identificar zonas sensibles, redefinir circuitos y, en resumen, establecer unas normas comunes adaptadas al grado de interés que la información de una empresa pueda despertar en terceros.

La seguridad es un aspecto vital para toda empresa (y muy rentable). Lamentablemente, su utilidad sólo se puede valorar cuando no existe y algo ocurre.

Es imprescindible que alguien asuma las funciones de coordinación de seguridad. Sólo así se puede permitir que hechos aislados lleguen a un mismo centro de análisis y toma de decisiones.

Audítese a sí mismo y a sus colaboradores respecto del cumplimiento de las normas. Realice regularmente reuniones de coordinación y motivación. No es conveniente que cite al culpable, pero comente los errores detectados: es la mejor forma de que todos puedan comparar lo ocurrido con su propio comportamiento y corrijan actitudes potencialmente peligrosas

Antes de descartar una determinada práctica por la incomodidad que representa, valore los riesgos que está asumiendo. Nunca podrá valorar de forma efectiva el nivel de seguridad de su sistema. En el mejor de los casos, lo único que podrá saber es que es insuficiente... pero entonces ya será tarde. Por ello, no permita que su equipo se relaje por la ausencia de incidencias: puede que no las haya habido precisamente por las medidas seguidas hasta ese momento.

Manténgase siempre al día: las fugas de información son como los ratones. Si no las ves no significan que no los haya. Si los ves, es que hay cientos de ellos.

Capacitación

Los sistemas y equipos son confiables, pero no infalibles, y son realmente las personas, entrenadas en los componentes y normas de la seguridad corporativa, las que harán la diferencia. Es indispensable que todo el personal tenga capacitación al nivel que requiera su posición y responsabilidades en la actuación de seguridad corporativa: seguir las normas de control de acceso, seguridad de la información sensitiva, detección de situaciones de riesgo, etc.

Por otra parte, una estrategia de capacitación que ha demostrado ser muy efectiva, y permite elevar la conciencia de seguridad de los empleados, se basa en impartir capacitación en autoprotección personal como parte del programa de desarrollo de RH de las empresas. Los empleados perciben el interés de la empresa en darles herramientas que les permitan vivir más seguros y, a su vez, este beneficio suele repercutir en una actitud más positiva e interactiva hacia los programas de seguridad de la empresa.

Objetivos del Sistema de Seguridad

Según la empresa Sistemas Operativos de Seguridad Privada Alcazar S.A. de C. V. Grupo S.O.S México, los objetivos de un sistema de seguridad son Identificar, mitigar y administrar efectivamente riesgos y vulnerabilidades que puedan amenazar la seguridad de la empresa, la capacidad de recuperación y la supervivencia de la organización. Esto implica una serie de acciones coordinadas y orientadas a un objetivo específico utilizando sus cuatro recursos o activos principales: recursos humanos, financieros, administrativos y operativos.

Estrategia de Seguridad Corporativa

Deben abordar unas medidas de seguridad acordes con los riegos a los que se enfrentan y, siempre, con una mentalidad preventiva más que reactiva. Por ello, el

primer elemento de una estrategia de seguridad es determinar el riesgo a controlar. Posteriormente, es necesario establecer una metodología de elección de los nuevos dispositivos de seguridad y de las nuevas tecnologías; definir una política de comunicación del sistema de seguridad; delimitar las métricas de implantación del proceso; determinar el modelo de negocio de la empresa y adecuarlo a las políticas de seguridad.

Acciones críticas

- Primero deberá hacerse un diagnóstico actualizado de amenazas, riesgos y vulnerabilidades. Un adecuado plan de seguridad inicia necesariamente con esta evaluación. Es una radiografía de cómo se encuentra el negocio o empresa en un momento y lugar determinado, desde un enfoque analítico integral.
- Deberá darse prioridad a debilidades, tomando en cuenta niveles de riesgo y el costo-beneficio de implementar mejoras.
- Otorgar autoridad a un responsable central de la seguridad. Un plan de seguridad corporativo debe tener, idóneamente, un responsable central y contar con el apoyo de la alta dirección.
- Formar una conciencia organizacional para "aceptar o comprar" las nuevas medidas de seguridad que se determine implementar.

Reporte e Investigación de Incidente

Es obligación de todos los trabajadores, reportar todo incidente del cual es testigo, facilitando, además, cualquier información necesaria para su inclusión en los Sistemas de Información disponibles

Cuando un trabajador sufra un accidente del trabajo, en la medida de lo posible, deberá dar aviso de inmediato a su jefe directo, quien proveerá el traslado del lesionado al centro de atención médica más cercano y se emitirá el documento de

Declaración Individual de Accidente del Trabajo a su organismo administrador del seguro contra accidentes del trabajo y enfermedades profesionales.

Programas de Gestión

Cuando las características de los trabajos / servicios lo requieran se definirá en las bases técnicas respectivas, existirá la necesidad que la empresa presente un Programa de Gestión, según formato que defina y que incluya los temas de seguridad, salud ocupacional, medio ambiente y calidad.

Actividades desarrolladas para el sistema de seguridad corporativa

Análisis de Vulnerabilidades

Identificación de vulnerabilidades

Para evaluar las distintas vulnerabilidades, se van a seguir las mismas categorías usadas para el análisis de riesgos. La mayor parte de las intrusiones a los sistemas que se producen hoy en día se deben a la explotación de vulnerabilidades, por ello es de vital importancia poder identificar todas aquellas vulnerabilidades susceptibles de ser aprovechadas por una amenaza, para evitar que ésta llegue a materializarse. La vulnerabilidades pueden deberse a fallos de seguridad de la propia empresa o fallos de seguridad en los productos suministrados por terceras empresas.

Vulnerabilidades relacionadas con desastres naturales

Los desastres naturales pueden llegar a ser, como se ha visto en el capítulo 5, amenazas muy graves para la empresa en el caso de que llegasen a materializarse en su tipo de impacto más alto.

Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Terremotos.
- Inundaciones.

Se pueden identificar las siguientes vulnerabilidades:

- Falta de políticas de Backup.

Vulnerabilidades relacionadas con amenazas estructurales

Las amenazas debidas a fallos estructurales son muy graves debido a que afectarían a todos los activos de la empresa provocando graves problemas de continuidad para la misma.

Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Incendios.
- Cortes eléctricos.
- Agua.
- Comunicaciones.

Se pueden identificar las siguientes vulnerabilidades:

- Falta de detectores de humos.
- Falta de políticas de Backup.
- Falta de dispositivos SAI que garanticen el suministro eléctrico.
- Dependencia exclusiva de un único proveedor de comunicaciones.

Vulnerabilidades relacionadas con el Hardware

Los problemas con el Hardware afectan directamente a los procesos informáticos de la empresa lo que puede provocar graves problemas en el transcurso normal de los negocios de la empresa.

Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Fallo de servidores.
- Fallo de estaciones PC
- Fallo de portátiles.

Se pueden identificar las siguientes vulnerabilidades:

- Falta de políticas de Backup.
- Falta de dispositivos SAI que garanticen el suministro eléctrico.

Vulnerabilidades relacionadas con el Software

Los fallos y errores de Software son muy perjudiciales, y son éstos los que más fácilmente pueden llegar a producirse si no se tiene cuidado con su correcto mantenimiento.

Las vulnerabilidades del Software son las más sensibles de ser aprovechadas por amenazas para infligir algún tipo de daño dentro de una organización.
Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Errores en los Sistemas Operativos.
- Errores en las Bases de Datos.

- Errores en las aplicaciones.
- Errores en los elementos de seguridad.

Se pueden identificar las siguientes vulnerabilidades:

- Mala actualización de los sistemas antivirus, firewalls y demás Software de seguridad
- Mala actualización de Software de gestión.
- Se dispone de Software elaborado a medida para la empresa por personal externo a ésta, pero que no responde adecuadamente del mantenimiento del mismo.

Vulnerabilidades relacionadas con las redes de comunicación

Las redes de comunicación son uno de los elementos más vulnerables a ser explotados por una amenaza, si no se cuida correctamente su mantenimiento y protección.

Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Red interna.
- Sistemas de seguridad de las comunicaciones
- Redes públicas ajenas.

Se pueden identificar las siguientes vulnerabilidades:

- Dependencia exclusiva de un único proveedor de comunicaciones.
- Bajo nivel de seguridad a la hora de realizar accesos a la red interna de la empresa.
- Mala actualización de Software de seguridad.

- No disponer de una red interna para realizar las comunicaciones dentro de la empresa y poder acceder a información interna sin necesidad de salir al exterior.

Vulnerabilidades relacionadas con las copias de seguridad

Para el correcto mantenimiento de la información generada por la empresa es recomendable que ésta sea replicada en diferente formato y en diferente lugar de donde se ha generado para salvaguardarla.

Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Fallos en los soportes de copias de seguridad. Se pueden identificar las siguientes vulnerabilidades:
- No existe una política de copias de seguridad por lo que una pérdida de datos sería irreparable.

Vulnerabilidades relacionadas con la información

La información es el activo más importante con que cuenta la empresa y por lo tanto en donde se debe poner más atención para evitar que tenga vulnerabilidades.

Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Ficheros.
- Procedimientos de seguridad de la información.
- Planes de contingencia.

Se pueden identificar las siguientes vulnerabilidades:

- No existen políticas de backup de la información.
- No existe una ubicación centralizada de almacenamiento de la información; ésta se encuentra repartida en los diferentes equipos de la empresa.
- No existen políticas ni medios de cifrado de la información crítica.
- No existen planes de contingencia para casos de pérdidas de información

Vulnerabilidades relacionadas con el personal

El personal de la empresa es una de las vulnerabilidades más importantes que puede tener una organización debido a que es un punto de fuga de información o un foco de ataques a la organización. Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Errores y ataques de personal interno.
- Errores y ataques de personal externo.

Se pueden identificar las siguientes vulnerabilidades:

- No existe una política de contraseñas para el acceso a los equipos.
- No existe una política de restricción de acceso a los datos.

Vulnerabilidades relacionadas con el patrimonio

Proteger los activos de la empresa ante terceros o pérdidas accidentales, es de vital importancia para no sufrir pérdidas graves de activos. Teniendo en cuenta las categorías empleadas para llevar a cabo el análisis de riesgos:

- Robo.

- Pérdida no intencionada de activos.

Se pueden identificar las siguientes vulnerabilidades:

- En la empresa existe un buen sistema de seguridad física que evita la pérdida de activos debido a robos, pero los sistemas Software de seguridad no están lo suficientemente bien adaptados a las necesidades de la empresa, conforme lo señala **Jorge Colinas (2008)**.

Medidas de seguridad

A la hora de realizar el análisis de la empresa, se han detectado ciertas vulnerabilidades graves como por ejemplo que no exista un replicado de la información, que no existan políticas de acceso a la información o la más importante, que los responsables de la empresa no tengan conciencia de la importancia de dotar a su empresa de unas adecuadas medidas de seguridad para proteger la información de la misma. Para conseguir reducir el riesgo de la empresa se van a detallar las medidas que se deberán emplear para conseguir que consiga ponerse al día en la seguridad de su información y elementos informáticos.

Dentro de las medidas a emplear para eliminar las vulnerabilidades y dotar a la empresa de una seguridad adecuada, se pueden distinguir varios tipos:

- Medidas preventivas: Medidas que se deberán implantar en la empresa para prevenir la posible explotación de una vulnerabilidad por parte de una amenaza.
- Medidas correctoras: Medidas que se deberán implantar en la empresa para corregir problemas o fallos debidos a amenazas que se han materializado.
- Riesgos asumibles: Pueden existir vulnerabilidades de la empresa que no sean sensibles a que un riesgo las explote, por lo que esa vulnerabilidad no es

necesario que sea tenida en cuenta a la hora de establecer las medidas de seguridad.

Medidas aplicadas a desastres naturales

A la hora de establecer medidas para proteger a la empresa de daños debidos a desastres naturales hay que tener en cuenta que no se puede controlar que lleguen, o no, a materializarse por lo que la empresa está expuesta a ellos y únicamente se pueden establecer medidas preventivas para intentar minimizar en lo posible el daño.

Medidas preventivas a adoptar dentro de la empresa:

- Instalación de dispositivos de protección de líneas eléctricas contra sobrecargas.
- Instalación de dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para garantizar el suministro eléctrico en caso de caída del sistema eléctrico general.
- Realización periódica de copias de Backup localizadas en servidores externos a la empresa.

Aunque antes se ha comentado que para tratar los desastres naturales sólo se pueden establecer medidas preventivas, la realización de copias de Backup se puede incluir también dentro de medidas correctoras.

Medidas aplicadas a problemas estructurales

Los posibles daños estructurales que se den en la empresa, aún siendo ajenos a la propia empresa sí pueden ser controlados mediante revisiones periódicas o mediante la contratación de servicios alternativos.

Medidas preventivas a adoptar dentro de la empresa:

- Revisión periódica de la instalación eléctrica.
- Instalación de dispositivos automáticos de extinción de incendios.
- Distribución de extintores a lo largo de toda la dependencia de la empresa, en especial cerca de elementos informáticos críticos.
- Instalación de dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para garantizar el suministro eléctrico en caso de caída del sistema eléctrico general.
- Contratación de dos líneas exteriores con suministradores de internet para garantizar siempre una conexión mínima a la red.

Medidas correctoras a adoptar dentro de la empresa:

Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.

- Riesgos asumibles en la empresa:
- Pérdida de las comunicaciones durante un periodo inferior a 24 horas.

Medidas aplicadas a problemas de Hardware

En el análisis realizado dentro de la empresa se han detectado varios fallos en el correcto mantenimiento y seguridad del equipamiento Hardware disponible, sobre todo debido a la ausencia de un sistema de almacenamiento centralizado, lo que pone en grave riesgo la integridad de la información almacenada dentro de dicho Hardware.
Algunas medidas aplicables para evitar pérdidas:

Medidas preventivas a adoptar dentro de la empresa:

- Instalación de un servidor de almacenamiento centralizado donde se almacene toda la información generada dentro de la empresa y que garantice un acceso adecuado, y seguro, a la misma cuando sea necesario.
- Disponer de copias de respaldo almacenadas en servidores exteriores a la empresa para prevenir posibles fallos de Hardware.
- Dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para evitar posibles fallos de los equipos debidos a cortes de energía repentinos.
- Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.

Medidas correctoras a adoptar dentro de la empresa:

- Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.
- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.

Riesgos asumibles en la empresa:

- Fallo en alguna estación PC o portátil durante un periodo inferior a 24 horas.

Medidas aplicadas a problemas de Software

El Software es el elemento más crítico de la empresa, pues debido a la falta de concienciación de seguridad de los responsables de la misma; los elementos Software que componen los activos de la empresa no están siempre correctamente actualizados y preparados para evitar posibles pérdidas de información no deseadas.

Medidas preventivas a adoptar dentro de la empresa:

- Realizar periódicamente, o cuando sea requerido por el distribuidor del Software, las actualizaciones oportunas para mantener al día los distintos programas y Sistemas Operativos.
- Instalación de bases de datos centralizadas donde se almacenen todos los datos importantes generados por la empresa para facilitar el almacenamiento, accesibilidad y seguridad de los datos.
- Disponer de Software de calidad y debidamente revisado.
- Establecer una política de contraseñas para acceder a los diferentes equipos de la empresa.

Medidas correctoras a adoptar dentro de la empresa:

- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.

Medidas aplicadas a problemas de red

La red es uno de los elementos más sensibles de la empresa, puesto que dentro de la misma no son conscientes de lo perjudicial que puede llegar a ser un ataque exterior y tampoco saben aprovechar las oportunidades que ésta puede proporcionar.

Medidas preventivas a adoptar dentro de la empresa:

- Montaje de una red interna en la empresa para garantizar que todas las comunicaciones internas y de carácter confidencial no salen de la estructura de la propia empresa.
- Mantener correctamente instalados y actualizados los sistemas de seguridad Software de los que dispone la empresa.

- Instalación en la totalidad de equipos de la empresa igual Software de seguridad que garantice la seguridad de los equipos.
- Establecimiento de políticas de seguridad de acceso a la red mediante el empleo de contraseñas.
- Instalación de un Router de acceso gestionable, más adecuado para la empresa que el proporcionado por la empresa suministradora del servicio.
- Establecer una correcta configuración de seguridad para la red inalámbrica que evite accesos indeseados.

Medidas correctoras a adoptar dentro de la empresa:

- Disponer de un correcto servicio de mantenimiento por parte de la empresa suministradora de servicios de comunicaciones que aseguren una rápida reparación y restablecimiento del servicio en caso de problemas con la línea.
- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.

Riesgos asumibles en la empresa:

- Fallo en los sistemas de comunicación de red durante un periodo no superior a 24 horas.

Medidas aplicadas a problemas de las copias de seguridad

La política de copias de seguridad es sin duda el talón de Aquiles de la empresa, pues dentro de la misma no se dispone de ningún sistema que garantice que se realicen copias de los datos críticos, ni que estas copias estén a salvo y replicadas en algún sistema de almacenamiento exterior a la empresa.

En este punto, también se detecta una falta de concienciación de los responsables de la empresa de lo importante que resulta tener la información replicada. Como nota de la importancia de este punto cabe reseñar que durante la elaboración del presente proyecto se perdieron en la empresa los datos fiscales que se encontraban informatizados del último año.

Medidas preventivas a adoptar dentro de la empresa:

- Instalación de un servidor centralizado de copias de seguridad en el cual se almacenen periódicamente copias de los datos actualizados.
- Realización periódica de copias de seguridad de los datos, en especial de los datos críticos, generados en la empresa.
- Realización periódica de copias de Backup localizadas en servidores externos a la empresa para garantizar la disponibilidad de los datos ante cualquier contratiempo en la empresa.
- Medidas correctoras a adoptar dentro de la empresa:
- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.

Medidas aplicadas a problemas con la información

La información es uno de los activos más importantes con los que cuenta la empresa y por tanto uno de los más críticos y que más habría que proteger.
Medidas preventivas a adoptar dentro de la empresa:

- Disponibilidad de copias de seguridad de los ficheros más importantes en diferentes soportes.
- Instalación de bases de datos centralizadas donde se almacenen todos los datos importantes generados por la empresa para facilitar el almacenamiento, accesibilidad y seguridad de los datos.

- Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.
- Establecimiento de planes de contingencia para salvaguardar la información y evitar daños o pérdidas de la misma.

Medidas correctoras a adoptar dentro de la empresa:

- Seguimiento de los procedimientos de seguridad establecidos para cada caso.
- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos
- Seguimiento del plan de contingencia especificado para cada caso.

Medidas aplicadas a problemas con el personal

En cualquier organización el personal es un punto crítico pues un empleado descontento puede provocar graves daños desde dentro de la organización. Cabe recordar que el 80% de los ataques informáticos que sufren las empresas proceden de dentro de la misma. En este caso un ataque desde dentro no es aplicable pues el personal que trabaja en la empresa es a la vez dueño de la misma y no realizará acciones conscientes que dañen a su propia empresa; aún así, como se ha comentado ya con anterioridad, el personal está muy poco concienciado con disponer de una adecuada seguridad y política de respaldo dentro de la empresa para garantizar la salvaguarda de su información.

Medidas preventivas a adoptar dentro de la empresa:

- Conseguir una adecuada concienciación del personal de la empresa sobre lo importante que es mantener un cierto nivel de seguridad en los procesos que se realizan dentro de la empresa. Así como establecer una adecuada política de respaldo de información.

- Disponibilidad de copias de seguridad de los ficheros más importantes en diferentes soportes.
- Establecer una política de contraseñas para el acceso a los recursos del sistema.

Medidas correctoras a adoptar dentro de la empresa:

- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.
- Realización de cursos de concienciación sobre la importancia de la seguridad de los datos para el personal de la empresa.

Medidas aplicadas a problemas con el patrimonio

En cualquier momento se puede estar sujeto a un robo o a una pérdida no intencionada de activos que provoque un problema de disponibilidad de datos importantes o una pérdida irrecuperable de los mismos.

Medidas preventivas a adoptar dentro de la empresa:

- Disponibilidad de copias de seguridad de los ficheros más importantes en diferentes soportes.
- Disponer de un completo inventario de todos los activos de la empresa.
- Tener la alarma conectada cuando no hay personal dentro de las instalaciones de la empresa.

Medidas correctoras a adoptar dentro de la empresa:

- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.

Medidas aplicadas a problemas provocados por otros riesgos

Otros factores que pueden afectar a la seguridad de los activos de la empresa pueden ser problemas de terrorismo, problemas con la imagen de la empresa, problemas de solvencia de los servicios externos, etc.

Medidas preventivas a adoptar dentro de la empresa:

- Disponer de copias de respaldo almacenadas en servidores exteriores a la empresa.
- Uso de Software comercial que asegure actualizaciones y mantenimiento con periodicidad.

Medidas correctoras a adoptar dentro de la empresa:

- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.
- Trabajar únicamente con proveedores de probada solvencia y que garanticen una rápida reparación y restitución del servicio en caso de fallos.

6.7. Metodología.

Tabla 38: Modelo Operativo

FASES	ETAPAS	METAS	ACTIVIDADES	RECURSOS	RESPONSABLE	TIEMPO
Inicial	**Sensibilización**	Socialización del proyecto con las autoridades y el personal de SRI Presentar la propuesta con las autoridades del SRI.	Presentación Socialización Discusión del proyecto Diálogos abiertos con el equipo de trabajo	Diseño del proyecto de la factibilidad propuesta Diseño preliminar del sistema	Dra. Mercy Solis	Mayo 2011 Julio 2011
Inicial	**Planificación**	Realizar el plan operativo a cumplir para la ejecución del proyecto	Diseño del cronograma de actividades.	Materiales de oficina. Diseño del proyecto de la factibilidad propuesta Computador.	Dra. Mercy Solis	Mayo 2011 Julio 2011

Central	**Implementación**	Ejecutar el cronograma de actividades planificadas para la realización del proyecto	Ejecución: ➢ Presentación de la propuesta ➢ Análisis riesgos ➢ Reuniones de consenso ➢ Realización de diseño preliminar ➢ Revisión de expertos ➢ Diseño del sistema definitivo ➢ Desarrollo de las actividades previstas en el Sistema de Seguridad Corporativa	Materiales de oficina. Diseño del proyecto de la factibilidad propuesta Computador.	Dra. Mercy Solis	Segundo Semestre 2011
Final	**Evaluación**	Comprobar los logros que se ha conseguido con la ejecución del proyecto	✓ Encuestas ✓ Entrevistas. ✓ Observación. ✓ Sondeos de opinión	Diseño del proyecto de la factibilidad propuesta	Dra. Mercy Solis	Evaluación permanente Indefinido

6.8. Administración

Institución: Servicio de Rentas Internas (SRI)

6.9. Previsión de la evaluación

Tabla 39: Evaluación

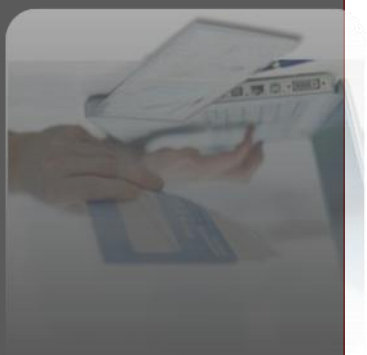
PREGUNTAS BASICAS	EXPLICACIÓN
¿Quiénes solicitan evaluar?	✓ Personal del SRI (Servicio Rentas Internas) ✓ Jefes Departamentales ✓ Autoridades del SRI ✓ Comunidad en general
¿Por qué evaluar la propuesta?	Para saber y analizar que estrategias se han cumplido, y en cuales ha existido más dificultades para su realización, para establecer la efectividad, determinando sus alcances y limitaciones
¿Para qué evaluar?	Para establecer si los objetivos y metas establecidos se han cumplido en forma satisfactoria y mejorar procesos, rediseñar actividades, optimizar recursos, establecer procesos más funcionales.
¿Qué evaluar?	Se evaluará la metodología utilizada, las metas establecidas a corto y mediano plazo, las principales actividades implementadas, el conocimiento referido sobre Seguridad Corporativa.

¿Quién evalúa?	✓ Personal del SRI (Servicio Rentas Internas) ✓ Jefes Departamentales ✓ Autoridades del SRI ✓ Comunidad en general
¿Cuándo evaluar?	La evaluación será permanentemente, estableciéndose el impacto de la propuesta en periodos trimestrales y realizar otra evaluación total en forma semestral, cada año se evaluará el proyecto analizando las metas cumplidas.
¿Cómo evaluar?	Mediante una investigación en la provincia sobre la ejecución del proyecto con: ✓ Encuestas Entrevistas. ✓ Observación. ✓ Sondeos de opinión ✓ Correos electrónicos
¿Con qué evaluar?	Con los instrumentos para la investigación: una grabadora, cuestionario de preguntas, guías de entrevista, auto –e valuación empresarial, liderazgo y observación, grupos focales.

Diseño del

Sistema de Seguridad Corporativa para el Servicio de Rentas Internas Ambato

Mercy Solis Pazmiño
Universidad Técnica de Ambato



1. Servicio de Rentas Internas Regional Centro Uno
2. La Seguridad Corporativa
3. Auditoría Forense
4. Sistema de Seguridad Corporativa
5. Ámbitos de la Seguridad Corporativa
6. Implementación y Control
7. Base Legal
8. Anexos

1. SERVICIO DE RENTAS INTERNAS REGIONAL CENTRO UNO

ANTECEDENTES.-

El Servicio de Rentas Internas es una Institución Pública creada mediante Ley No.041 del 13 de noviembre de 1997, publicada en el Registro Oficial No. 206 del 2 de Diciembre del mismo año.

MISIÓN.-

Promover y exigir el cumplimiento de las obligaciones tributarias, en el marco de principios éticos y legales, para asegurar una efectiva recaudación que fomente la cohesión social.

VISIÓN.-

Ser una institución que goza de confianza y reconocimiento social por hacerle bien al país. Hacer bien al país por nuestra transparencia, modernidad, cercanía y respeto a los derechos de los ciudadanos y contribuyentes. Hacer bien al país porque contamos con funcionarios competentes, honestos, comprometidos y motivados. Hacer bien al país por cumplir a cabalidad la gestión tributaria, disminuyendo significativamente la evasión, elusión y fraude fiscal.

VALORES.-

Vocación de Servicio.- La vocación de servicio de los funcionarios del SRI es el atributo por el cual somos reconocidos por nuestra comunidad estratégica, ya que refleja un modelo de gestión pública orientada al cliente, que promueve el cumplimiento voluntario de sus obligaciones tributarias.

Honestidad, Ética, y Probidad. - Actuamos siempre con base en la verdad y en la auténtica justicia, la práctica de la moral y la rectitud en el logro de los objetivos institucionales. La integridad de nuestras actuaciones genera confianza y credibilidad en la ciudadanía.

Compromiso. Los funcionarios del SRI son conscientes de su valioso aporte para la Administración Tributaria, por lo cual se comprometen con la misión institucional, entendiendo que su esfuerzo le hace bien al país y contribuye en la construcción de una verdadera cohesión social.

Equidad. Todos los contribuyentes merecen ser asistidos o gestionados con los mismos derechos y garantías. Los funcionarios de la Administración Tributaria en el ejercicio de sus facultades, son técnicos e imparciales.

Respeto. El SRI es una institución valorada por la sociedad, por su profundo sentido de respeto a los derechos de los ciudadanos, al uso de los recursos públicos con rendición de cuentas y por las relaciones cordiales entre sus funcionarios.

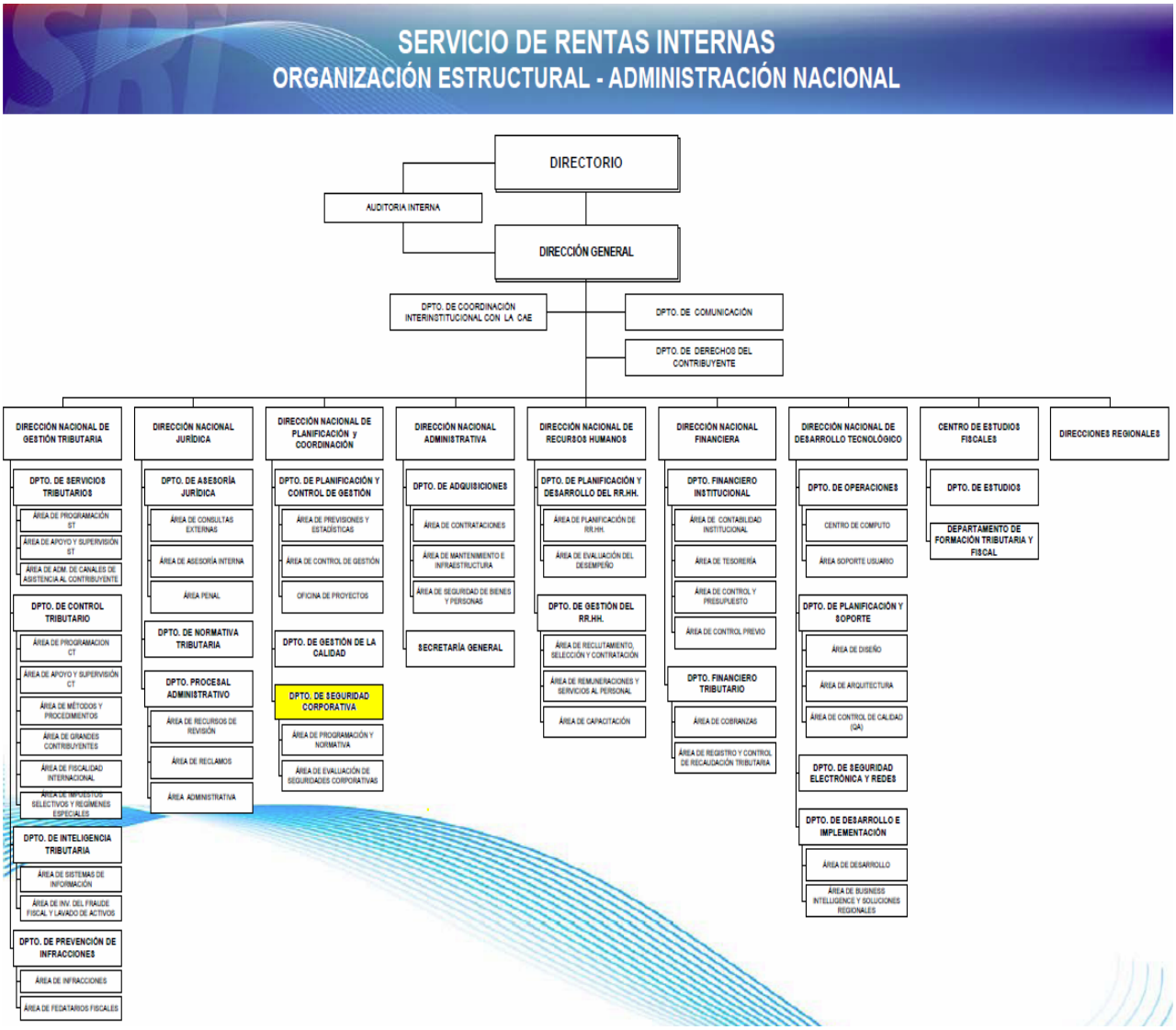
Trabajo en equipo. Somos un equipo sólido, motivado, cohesionado y respetuoso de las ideas, donde no existen barreras u objetivos divergentes. Tenemos una única misión que nos permite lograr los objetivos que la sociedad demanda. Nuestro esfuerzo en conjunto genera sinergias que nos facilitan alcanzar nuestra visión compartida.

ESTRUCTURA ORGANIZATIVA.-

La institución está conformada por una Administración Central que trabaja desconcentradamente con ocho Direcciones Regionales que incluyen a su vez Direcciones Provinciales y delegaciones zonales.

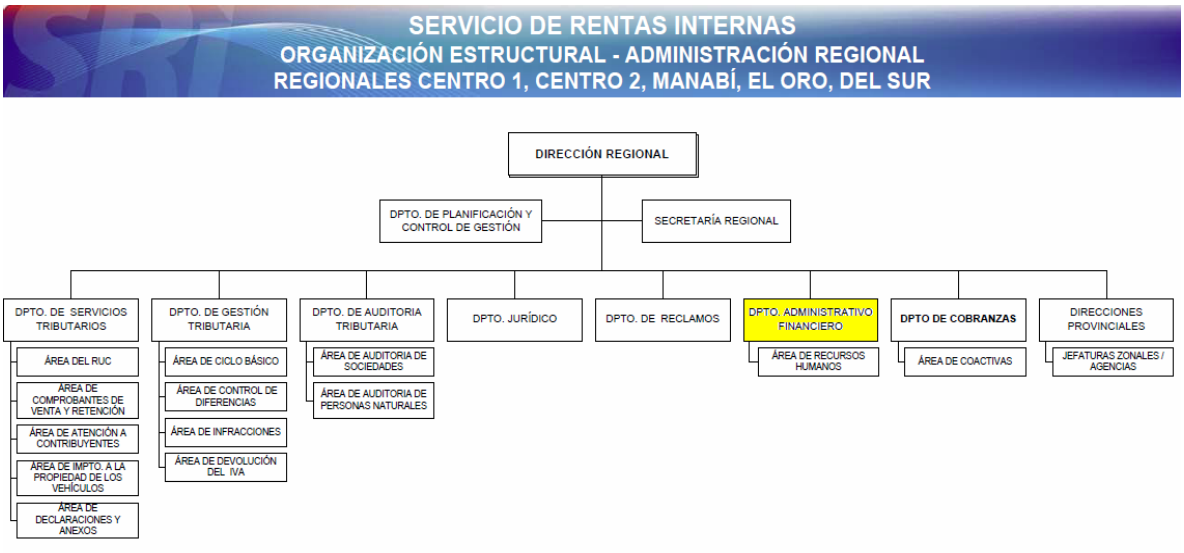
La Administración Central con jurisdicción en todo el país es la encargada de establecer los lineamientos estratégicos, objetivos, políticas, procesos y procedimientos, así como vigilar su cabal aplicación y cumplimiento.

Dentro de la estructura orgánica funcional aprobada por el Directorio de la Institución, la Dirección Regional Centro Uno comprende las provincias de Tungurahua, Cotopaxi y Pastaza, la sede principal es la ciudad de Ambato. Cuenta con tres agencias zonales: Baños, Agencia Sur (Ambato) y la Maná (Cotopaxi).



Tal como se puede apreciar en la Organización Estructural de la Administración Nacional, existe dentro de la Dirección Nacional de Planificación y Coordinación, el Departamento de Seguridad Corporativa, encargado de establecer los lineamientos de control y seguridad a nivel nacional.

Dentro de la Administración Regional, si bien no existe como definición un departamento o área de Seguridad Corporativa, las funciones de seguridad y control Regional, conforme el orgánico funcional, le corresponde al Departamento Administrativo Financiero.



2. LA SEGURIDAD CORPORATIVA

DEFINICIÓN.-

El término Seguridad Corporativa integra un conjunto de sistemas, elementos y recursos que dispone la organización y que están expuestos a diversos riesgos que pueden provocar pérdidas en diversos aspectos. Trata de establecer mecanismos, planes y otras acciones que minimicen riesgos.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización.

El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Alcance.-

El presente diseño del Sistema de Seguridad Corporativa aplica a la Dirección Regional Centro Uno del Servicio de Rentas Internas con sede en la ciudad de Ambato.

La Dirección Regional comprende los siguientes departamentos:

1. Servicios Tributarios

2. Gestión Tributaria
3. Auditoría Tributaria
4. Jurídico
5. Administrativo Tributario
6. Reclamos
7. Cobranzas

Adicionalmente cuenta con dos Direcciones Provinciales: Cotopaxi y Pastaza y dos Jefaturas Zonales en Baños y la Maná, además de la Agencia Sur-Ambato.

Los departamentos que conforman la Regional Centro Uno, administran, manejan y custodian información sensible que requiere de adecuados controles y seguridades para garantizar su integridad y buen uso, además de la adecuada conservación en el tiempo.

- **LA AUDITORIA FORENSE**

DEFINICIÓN.-

El término “forense” que proviene del latín “forensis” que significa “público y manifiesto” o “perteneciente al foro”; a su vez “forensis” se deriva de “fórum” que significa “foro”, “plaza pública”

Cuando en la ejecución de labores de auditoría (financiera, de gestión, informática, tributaria, ambiental, gubernamental) se detecten fraudes financieros significativos; y, se deba (obligatorio) o desee (opcional) profundizar sobre ellos se está incursionando en la denominada auditoría forense. La investigación será obligatoria dependiendo de: 1) el tipo de fraude; 2) el entorno en el que fue cometido; y, 3) la legislación aplicable. La labor de auditoría forense también puede iniciar directamente sin necesidad de una auditoría previa de otra clase, por ejemplo en el caso de existir denuncias específicas.

La auditoría forense es aquella labor de auditoría que se enfoca en la prevención y detección del fraude financiero; por ello, generalmente los resultados del trabajo del auditor forense son puestos a consideración de la justicia, que se encargará de analizar, juzgar y sentenciar los delitos cometidos (corrupción financiera, pública o privada).

La Auditoría Financiera Forense es relativamente nueva pero cada vez más importante. A raíz de la globalización se ha acentuado también el fenómeno de la corrupción, especialmente en la alta dirección (“crimen de cuello blanco”), con estructuras tan complejas como las utilizadas para el lavado de activos en sus diversas modalidades. El análisis de ello ha conducido a ver la auditoría financiera con otra perspectiva: los supuestos de empresa en marcha y buena fe, que conducen a la detección de irregularidades, hacen crisis frente a estos nuevos delitos.

RELACIÓN CON SEGURIDAD CORPORATIVA.-

Una sólida estructura de Seguridad Corporativa constituye un control interno adecuado y permite minimizar riesgos de cualquier naturaleza, y su efectividad se mide con los resultados de ejecución de una Auditoría Forense Integral.

Un sistema débil de control interno reflejado en la poca seguridad corporativa provoca una oportunidad a quien es propenso a cometer irregularidades de cualquier tipo.

El objetivo del presente diseño del sistema de Seguridad Corporativa para el Servicio de Rentas Internas de Ambato, es principalmente contar con un plan de seguridad que permita identificar en forma oportuna riesgos y minimizar los impactos que estos pudieran ocasionar sobre bienes tangibles e intangibles. Además se requiere contar con alertas tempranas que adviertan sobre riesgos latentes para impedir su progreso y evitar fraudes corporativos que afecten gravemente la imagen institucional.

- **SÍSTEMA DE SEGURIDAD CORPORATIVA.-**

Los sistemas informáticos de las empresas se encuentran repletos de soluciones de seguridad para proteger la información corporativa. Sin embargo, una Política de Seguridad mal definida o inexistente, entornos tecnológicos heterogéneos, instalaciones mal planificadas o personal técnico sin formación específica determinan un escenario deshilachado y mal engranado. Es necesario complementar las herramientas de seguridad con sistemas que las controlen e integren desde un punto de vista lógico.

La actualización y reingeniería de los procesos de seguridad existentes son también importantes a fin de implementar y coordinar todo el sistema de seguridad corporativa para el Servicio de Rentas Internas de Ambato.

La teoría organizacional moderna define al análisis de sistemas como la manera más adecuada de estudiar las organizaciones, utilizando como herramientas para dicho estudio a una base analítica conceptual caracterizado por la confianza en la observación de los hechos y la naturaleza sintetizadora e integradora.

A su vez, tal como se ha dicho, toda organización está compuesta por varios subsistemas interdependientes, formulados o no, que se asocian entre sí en un único suprasistema. Pero para ello la organización debe seleccionar un estilo de gestión que le sea útil, para llevar adelante todos los subsistemas que la constituyen. De este modo si bien existen estándares, reglas y demás cada organización es peculiar en su instrumentación, implantación y desarrollo por lo que en última instancia no existen sistemas sino organizaciones.

El Sistema de Gestión Integrado se apoya en documentación escrita, cuya función es guiar y controlar todas las acciones para el logro de los objetivos y su propósito principal es asegurar que todo el personal tanto el de Organización como de los contratistas, está utilizando los mismos procedimientos e instrucciones de trabajo en una misma forma consistente.

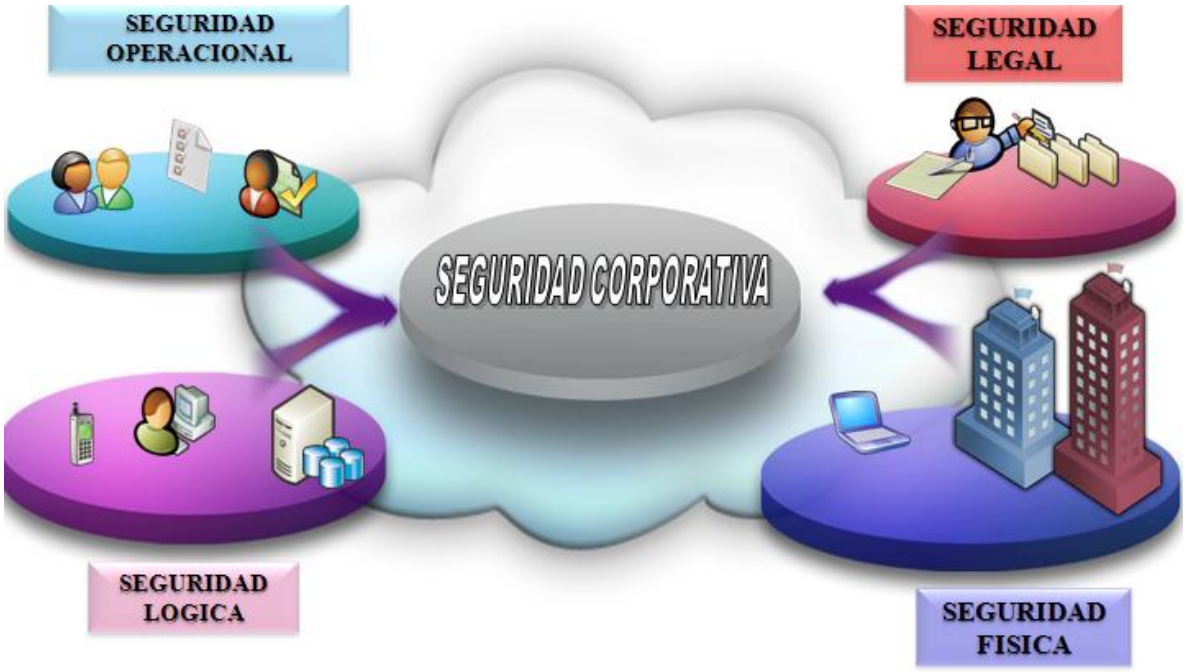
Los principales documentos son:

- El manual de gestión integrado, que describe en forma genérica la estructura del sistema de gestión ambiental y de seguridad y hace referencia a los documentos del mismo.
- Los manuales de procedimientos especifican la forma de realizar las actividades vinculadas al sistema, las distintas responsabilidades, los mecanismos de control y los registros obtenidos.
- Los procedimientos de gestión son los que regulan el funcionamiento y estructura del sistema; los operativos controlan las actividades y procesos propios del área y se vinculan con los efectos ambientales significativos.
- El plan de contingencia debe describir todos los mecanismos a seguir ante situaciones de emergencias.

- Los registros fundamentales para el sistema son: Registro de normas aplicables, el registro de **aspectos/impactos físicos** y el registro de **aspectos/impactos de salud** (peligros/riesgos).

- **ÁMBITOS DE LA SEGURIDAD CORPORATIVA.-**

La Seguridad Corporativa abarca una gama muy variada y amplia de aspectos que una organización debe considerar, tal como se muestra a continuación:



Sin embargo, conforme el análisis efectuado y considerando la estructura funcional del Servicio de Rentas Internas de Ambato, se consideran para el presente diseño dos ámbitos de acción que incorporan todas las actividades desarrolladas, estos son:

1. Seguridad Tecnológica

2. Seguridad Física

Es importante mencionar que la Organización deberá identificar y cuantificar las operaciones que realiza y enmarcarlas dentro de uno de los niveles de seguridad señalados.

SEGURIDAD TECNOLÓGICA.-

Se identifican las principales seguridades y controles establecidos en este ámbito de la Seguridad Corporativa.

Acceso a los Sistemas de Información

Objetivos.-

- Optimizar y estandarizar los procesos de administración de accesos de funcionarios del SRI (usuarios finales y usuarios técnicos) a la infraestructura tecnológica;

- Desarrollar políticas y procedimientos en base a estándares de seguridad relacionadas al proceso de administración de accesos;

- Diseñar e implementar mecanismos de control, monitoreo y gestión en la ejecución del proceso de administración de accesos lógicos;

- Documentar el análisis, diseño, desarrollo e implementación del proceso de administración y control de accesos lógicos a la infraestructura tecnológica de la Institución.

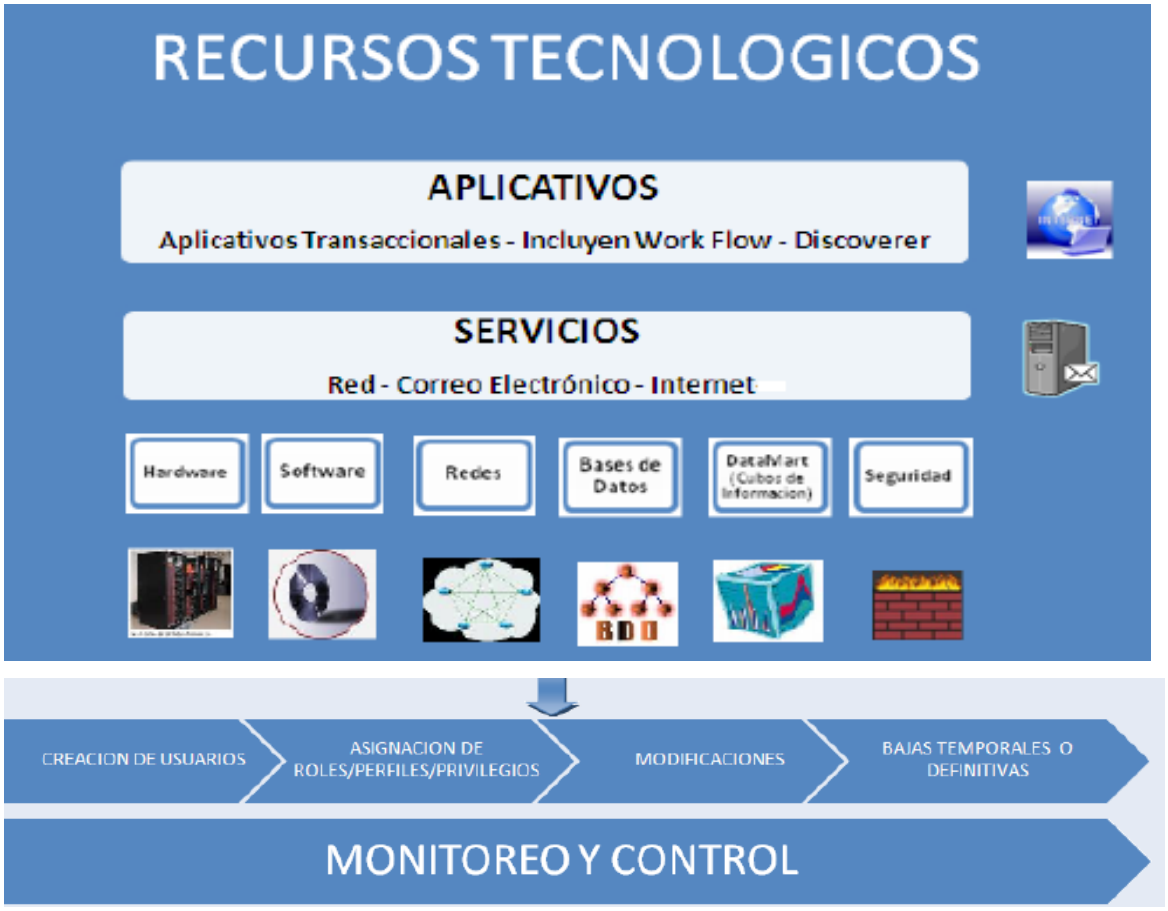
Documentos a generar.-

- Definir el procedimiento para solicitar acceso a los Sistemas de Información.
- Éste debe constar como anexo del Documento de Seguridad y debe estar actualizado por el centro.

- El Responsable Funcional de Aplicación debe ser la figura a la que el usuario/profesional consulte la mayoría de sus dudas respecto de los datos de carácter personal.

- Las credenciales de un usuario relacionan a éste con sus acciones en los Sistemas de Información, Responsabilidades.

Se debe considerar todos los aspectos: transacciones, usuarios y agentes que participan en los distintos procesos operacionales, además de los bienes tangibles e intangibles, tal como se muestra en el siguiente gráfico:



<u>Encriptación de la Información</u>

Objetivos.-

- Implementar el proceso de encriptación que permita proteger la información institucional de accesos no autorizados

- Desarrollar las políticas y procedimientos de encriptación en base a estándares de seguridad.

Documentos a generar.-

- ✓ Solución de encriptación implementado y operativa en los computadores de escritorio y/o portátiles que almacenen información institucional sensible.

- ✓ Políticas y procedimientos documentados relacionados a la encriptación de información institucional.

- ✓ Mecanismos técnicos de control y monitoreo del proceso de encriptación

Dentro de los departamentos que administran y manejan información confidencial se encuentran el departamento de Auditoría Tributaria, Gestión Tributaria y Jurídico principalmente, estos deberán tener prioridad en el proceso de encriptación que garantice una adecuada salvaguarda de esta información sensible. El proceso se muestra a continuación:

<u>Respaldos de Información.-</u>

Objetivos.-

La ejecución del proyecto de respaldos de información almacenada en computadores de escritorio y/o portátiles, tiene los siguientes objetivos:

- Diseñar e implementar el proceso de respaldos de información institucional.
- Desarrollar las políticas y procedimientos, en base a estándares de seguridad, relacionados al proceso de respaldos de información institucional.
- Implementar mecanismos técnicos para la obtención de respaldos automáticos de información institucional almacenada en los computadores de escritorio y portátiles asignadas a funcionarios de la institución.

Documentos a generar.-

- ✓ Solución de respaldos automáticos para computadores de escritorio y portátiles, que brinde el servicio a 1200 usuarios.

- ✓ Políticas y procedimientos documentados, relacionados a los respaldos automáticos de información institucional.

- ✓ Mecanismos técnicos de control y monitoreo durante la ejecución de procesos de respaldo de información.

Otras Seguridades Tecnológicas.-

Objetivos.-

- Definir los lineamientos de seguridad en las operaciones tecnológicas ejecutadas por usuarios
- Limitar el acceso a información restringida

Seguridad en las conexiones a Internet.

- Políticas en el Firewall
- VPN
- Detección de intrusos

Seguridad en la infraestructura de comunicaciones.

- Routers
- Switches
- Firewall
- Hubs
- RAS

Seguridad en Sistema Operacionales
Correo Electrónico
Seguridad en las aplicaciones
Auditorías de Seguridad de Sistemas de Información

Documentos a generar.-

- ✓ Políticas de Uso y Acceso a Información

- ✓ Procedimientos, Resoluciones, Circulares de conocimiento general

Seguridad Física.-

La Seguridad Física involucra tanto al recurso humano y la infraestructura de las instalaciones donde desarrollan sus actividades.

Es indispensable que se identifiquen las principales amenazas y vulnerabilidades a los que se encuentran expuestos los activos físicos que integran la organización y que se pueden resumir en:

Los planes operativos implementados para la seguridad física deben comprender el compromiso de los altos directivos, administrar los riesgos identificados y mantener actualizaciones periódicas para garantizar su éxito.

Consideremos las siguientes seguridades en instalaciones:

- ✓ Tarjetas de identificación y acceso del personal a área restringidas

- ✓ Cerraduras en buen estado en todas las puertas, armarios y cajones. Si maneja documentos especialmente sensibles, adquiera una caja de seguridad para almacenar los mismos. Dichas llaves deberán estar en su poder y, en caso necesario, en el de su secretaria o colaborador de confianza. En previsión de emergencias, entregue una copia al responsable de seguridad, dentro de un sobre de seguridad cerrado y con su firma en la unión de la solapa con la bolsa, para su depósito en una caja de seguridad.

- ✓ Al abandonar su lugar de trabajo no deje sobre su escritorio papeles, documentos que contengan información importante.

- ✓ Bloquee el uso de su equipo de cómputo asignado cada vez que tenga que ausentarse de su oficina. Implementar bloqueos automáticos para equipos de computación.

- ✓ Uso de claves seguras y cambios periódicos de las mismas

- ✓ Disponga de destructora de documentación, de prestaciones adecuadas al volumen de los documentos que maneja. Utilice siempre para destruir copias o documentación reservada.

- ✓ Instalar alarmas y cámaras de video en áreas sensibles de acceso

- ✓ Uso adecuado de internet y redes sociales, no divulgue información de la Institución por sitios de acceso masivos

- ✓ Instalaciones eléctricas en adecuadas condicionadas (mantenimiento periódico)

- ✓ Planes de socialización y capacitación periódicas sobre los sistemas de seguridad implantados
- ✓ Identificar y documentar planes de seguridad por vulnerabilidades a desastres naturales:

Terremotos.
Inundaciones.
Erupción Volcánica

- ✓ Identificar y documentar planes de seguridad por vulnerabilidades estructurales:
  Incendios.
  Cortes eléctricos.
  Agua.
  Comunicaciones.

- ✓ Identificar y documentar planes de seguridad por vulnerabilidades de la información física:
  Espacios físicos adecuados
  Sistemas de ambiente adecuados
  Políticas de conservación y mantenimiento de archivos físicos
  Políticas de uso y préstamo de documentos archivados

- ✓ Inventariar riesgos en cada uno de los departamentos y mantener una actualización periódica a fin de minimizar sus impactos

Todas las vulnerabilidades y amenazas deben ser controladas con medidas preventivas y correctivas.

Las medidas preventivas serán aquellas que deberán implantarse en la empresa para prevenir la posible explotación de una vulnerabilidad por parte de una amenaza.

Las Medidas correctivas en cambio son las que se deberán implantar en la empresa para corregir problemas o fallos debidos a amenazas que se han materializado.

En resumen con la implementación de las seguridades físicas se pretende cubrir todos los riesgos posibles y minimizar su impacto, lo dicho se muestra en el siguiente gráfico:

- **IMPLEMENTACIÓN Y OPERACIÓN.-**

Finalizada la fase de diseño, se requiere poner en práctica una serie de elementos exigidos por las Normas. Estos se explican a continuación.

Estructura y Responsabilidad

El Sistema no podrá entrar en funcionamiento a menos que se establezca una estructura organizativa que permita la adecuada movilidad requerida.

Considerando la estructura organizacional del Servicio de Rentas Internas Ambato, la implantación y mantenimiento del sistema es responsabilidad del Departamento Administrativo Financiero y alcanza a todo el personal que cumple sus funciones en el lugar. Los departamentos operativos proveen a todo el personal de los medios que garanticen la formación y el adiestramiento adecuado para las tareas que cada uno desempeña. Las soluciones podrían ser otras, pero esta vía ha permitido un rápido desarrollo del Sistema y el cumplimiento de sus objetivos.

Mediciones y seguimiento.

Se refiere a todas aquellas acciones que se hacen en la operación y que permiten cubrir los requisitos legales en cuanto a medición de parámetros exigidos por las normas y regulaciones o bien, garantizar que los equipos y procesos asociados a la operación se encuentren a niveles de óptimo desempeño.

El centro integrador es el proceso y es quien debe focalizar la acción. El grupo auditor insiste en este aspecto de la Norma, porque al estar ligado a la integridad de la operación misma, posee un fuerte impacto en la verificación del buen funcionamiento del Sistema de Gestión

7. BASE LEGAL.-

- La Constitución de la República del Ecuador, aprobada en referéndum el 28 de septiembre de 2008 y publicada en el Registro Oficial 449 del 20 de octubre de 2008, en su artículo 211 dispone que le compete a la Contraloría General del Estado realizar el control de la utilización de los recursos

estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que disponen de recursos públicos

- La Ley Orgánica de la Contraloría General del Estado expedida mediante Ley 73 y publicada en el Registro Oficial Suplemento 595 de 12 de Junio del 2002, en la parte pertinente señala: "Art. 4.- Régimen de control de las personas jurídicas con participación estatal.- Para todos los efectos contemplados en esta Ley, están sometidas al control de la Contraloría General del Estado, las personas jurídicas y entidades de derecho privado, exclusivamente sobre los bienes, rentas u otras subvenciones de carácter público de que dispongan, cualesquiera sea su monto, de conformidad con lo dispuesto en el inciso segundo del artículo 211 de la Constitución Política de la República"

En el mismo cuerpo legal el Art. 6, señala: "Componentes del Sistema.- La ejecución del sistema de control, fiscalización y auditoría del Estado se realizará por medio de:

1.- El control interno, que es de responsabilidad administrativa de cada una de las instituciones del Estado a las que se refiere el artículo 2 de esta Ley; y,

2.- El control externo que comprende:

a) El que compete a la Contraloría General del Estado; y,
c) El que ejerzan otras instituciones de control del Estado en el ámbito de sus competencias"

El Art. 9 en la parte pertinente señala, " Concepto y elementos del Control Interno.- El control interno constituye un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales. Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, los riesgos institucionales en el logro de tales

objetivos y las medidas adoptadas para afrontarlos, el sistema de información, el cumplimiento de las normas jurídicas y técnicas; y, la corrección oportuna de las deficiencias de control.

El control interno será responsabilidad de cada institución del Estado, y tendrá como finalidad primordial crear las condiciones para el ejercicio del control externo a cargo de la Contraloría General del Estado.

Además la Ley Orgánica de la Contraloría en el Art. 12 indica: "Tiempos de control.- El ejercicio del control interno se aplicará en forma previa, continua y posterior:

a) Control previo.- Los servidores de la institución, analizarán las actividades institucionales propuestas, antes de su autorización o ejecución, respecto a su legalidad, veracidad, conveniencia, oportunidad, pertinencia y conformidad con los planes y presupuestos institucionales;

b) Control continuo.- Los servidores de la institución, en forma continua inspeccionarán y constatarán la oportunidad, calidad y cantidad de obras, bienes y servicios que se recibieren o prestaren de conformidad con la ley, los términos contractuales y las autorizaciones respectivas"

- La Ley de Creación del Servicio de Rentas Internas, creada mediante Ley No.41 publicada en el Registro Oficial 206 del 2 de diciembre de 1997, que en el artículo 1 dispone que: "..Créase el Servicio de Rentas Internas (SRI) como una entidad técnica y autónoma, con personería jurídica, de derecho público, patrimonio y fondos propios, jurisdicción nacional y sede principal en la ciudad de Quito. Su gestión estará sujeta a las disposiciones de esta Ley, del Código Tributario, de la Ley de Régimen Tributario Interno y de las demás leyes y reglamentos que fueren aplicables y su autonomía concierne a los órdenes administrativo, financiero y operativo"

  El mismo cuerpo legal en el artículo 17 señala: "Del control interno.- El Servicio de Rentas Internas establecerá los métodos y procedimientos propios de control interno, de conformidad con lo previsto en la Ley Orgánica de Administración Financiera y Control.

Se establecerá la Unidad de Auditoría Interna que efectuará el examen posterior de las operaciones financieras y administrativas de la entidad y presentará sus informes para conocimiento del Director General del Servicio de Rentas Internas, Directorio y Contralor General del Estado"

- Código de Ética, expedido mediante resolución general NAC-DGER2007-1350 el 29 de diciembre de 2007 y publicada en el Registro Oficial No.253 de 16 de enero de 2008, que busca consolidar un comportamiento moral y compromiso de todos los funcionarios, definido así en los artículos 4: "Compromiso personal de los servidores: Los servidores de la Administración Tributaria deben asumir la responsabilidad personal de conocer y promover el cumplimiento de los principios, valores y pautas contenidos en este Código, el cual será un referente para el fortalecimiento institucional y la promoción de la ética, al interior del SRI"

El artículo 15, respecto de la utilización de los bienes y recursos públicos, indica: "Uso de bienes y recursos públicos.- Los servidores del SRI utilizarán los bienes y recursos públicos institucionales, únicamente para actividades relacionadas con el desarrollo de actividades inherentes a la Administración Tributaria.

En el mismo código de ética el artículo 19, señala: "Uso de información para fines permitidos.- Es obligación del servidor utilizar la información a la que tiene acceso en razón de su trabajo, únicamente para los fines permitidos, conforme a la normativa y a las órdenes del servidor competente. De igual forma es deber del servidor abstenerse de acceder a la información que no le haya sido autorizada, asignada o permitida…"

El artículo 20 señala respecto de las políticas de uso de claves: "Cada servidor tendrá especial cuidado, uso y manejo de las claves y seguridades empleadas para acceder a la red de información electrónica institucional…"

Finalmente el artículo 22 se refiere a la prevención de revelación no autorizada, señalando que "El custodio de la información, debe realizar los esfuerzos necesarios para precautelar la seguridad y prevenir la revelación no autorizada de información del SRI" y el artículo 23 que indica sobre el uso de la información tributaria: "Los servidores no podrán revelar información tributaria referente a los contribuyentes, a servidores no autorizados…"

Acuerdo de Confidencialidad sobre Manejo de Información, asumido por todos los integrantes de la Organización, y regularizado mediante resolución general NAC-DGER2008-0987 del 7 de mayo de 2008.

ANEXOS.-

Suplemento Registro oficial No. 389, 25 de julio de 2008

"Art. 22 C.- Son funciones del Departamento de Seguridad Corporativa:

1. Establecer y mantener actualizado un sistema de seguridad institucional, en todos los ámbitos de la organización;

2. Promover el desarrollo de una cultura de prevención y mitigación oportuna de riesgos;

3. Promover la aplicación de metodologías de trabajo en las fases de planificación, ejecución, evaluación y actualización de las acciones de preservación y protección de los activos claves de la organización;

4. Informar los resultados del sistema de evaluación y control de las seguridades, recomendando las acciones de mejora continua;

5. Presentar al Comité de Seguridad Corporativa, para su aprobación, el Plan de Evaluación Anual a las Seguridades Corporativas, y monitorear su ejecución; y,

6. Evaluar las acciones desarrolladas por el personal del SRI, en el cumplimiento de las políticas y normas de seguridad corporativa."

BIBLIOGRAFIA

- ABRIL, Víctor Hugo, "Elaboración y Evaluación de Proyectos de Investigación", Programas de Maestría, Universidad Técnica de Ambato, 2008, 58p
- ANDRADE, Mario, "Control de los recursos y riesgos del Ecuador", Instituto de Auditores Internos, 2006, 68p
- BADILLO, Jorge, "Administración de Riesgos (ERM)", Seminario Taller, Servicio de Rentas Internas, Ambato, Ecuador, 2008, 50p
- BERNAL, César, "Metodología de la Investigación para Administración y Economía", primera edición; Editora Pearson Educación; Colombia; 2000; 259p
- CANO, Miguel y LUGO, Danilo; "Auditoría Forense en la Investigación Criminal del Lavado de Dinero y Activos"; Ecoe Ediciones; Bogotá – Colombia; 2005; p. 16, 20
- CERDA, Hugo, "La Investigación Total", Editorial el Búho, Bogotá; 1998
- CHIRIBOGA, Luis, "Dirección Técnico Financiero Ecuatoriano", 6ª. Edición; Editorial Universitaria; Quito; 2008; 179p
- COLINAS Ramírez Jorge, Plan de Seguridad para una Pequeña Empresa, Universidad Pontificia Comillas, Madrid, Septiembre del 2008
- ESTUPIÑÁN, Rodrigo; "Control Interno y Fraudes"; 1a. Edición 3a. reimpresión; ECOE Ediciones; 2004; 374p
- FRACICA, Germán, "Modelo de Simulación de Muestreo", Universidad de la Sabana, Bogotá; 1998
- HERNANDEZ, Roberto y otros; "Metodología de la Investigación", 3a edición; México; Editorial Mc Graw Hill; 2003; 689p
- HERRERA, Luis y otros; "Tutoría de la Investigación Científica"; Quito; Empresdane Gráficas Cía. Ltda.; 2004; 229p
- KELL, Walter y otros; "Auditoría Moderna", 3a edición; México; Editorial Continental; 1983; 715p
- LOZANO, Jorge; "Auditoría Interna, su enfoque"; 1ª. Edición; Ediciones contables administrativas; México; 1973; 67p

- MALDONADO, Milton, “Auditoría Forense: Prevención e Investigación de la Corrupción Financiera”; 1a. edición; Editora Luz de América; 2003; 314p
- MANTILLA, Alberto; “Auditoría 2005”; Ecoe Ediciones; Bogotá – Colombia; 2004; p. 708.
- YANEL, Blanco; “Manual de Auditoría y Revisoria Fiscal”; 2ª. Edición; Editora Roesga; Bogotá; 1987; 494p
- WILLINGHAM, John y otros; “Auditoría: Conceptos y Métodos”; 1ª. Edición; Editora Mc Graw Hill; 1982; 457p

- ATISAE, Gestión de Calidad, Seguridad y Medio Ambiente. España. www.atisae.com/calid.htm (Fecha de consulta: 17.04.2011)
- AVILA, Héctor, (2009). “Introducción a la Metodología de la Investigación”. (En línea) Disponible en: http://www.eumed.net/libros/2006c/203/1u.htm (Fecha de consulta: 7.06.2010)
- DE LA FUENTE, Leopoldo, (2009). "La Investigación”. (En línea) Disponible en: lfuente[arroba]yahoo.com (Fecha de consulta: 21.06.2010)
- FRIGO Edgardo, La Seguridad basada en el valor.- Foro de Profesionales Latinoamericanos de Seguridad, http://www.forodeseguridad.com/artic/segcorp/7205.htm. (Fecha de consulta: 14.04.2011)
- FUDIM, Pablo; Seminario de Auditoría Forense; Proyecto Si Se Puede; www.sisepuede.com.ec.; p. 6. (Fecha de consulta: 31.01.2011)
- ISMS FORUM SPAIN, (2009).” ISO 27000”(En línea) Disponible en: http://www.iso27000.es/ (Fecha de consulta: 21.06.2010)
- MEZA CASCANTE, Luis Gerardo, (2010). “El paradigma positivista y la concepción dialéctica del conocimiento”. (En línea) Disponible en: http://www.cidse.itcr.ac.cr/revistamate/ContribucionesV4n22003/meza/pag1.html (Fecha de consulta: 22.06.2010)

- RODRÍGUEZ Diofanor, Gestión empresarial de Seguridad, Los tres elementos clave de la Gestión Estratégica Empresarial, http://www.forodeseguridad.com/artic/segcorp/7207.htm (Fecha de consulta: 22.03.2011)
- TAMAYO TAMAYO, Mario, (2009). "El proceso de la investigación". (En línea) Disponible en: http://www.lafacu.com/apuntes/educacion/Metodologiadeinvestigacion/default.htm
(Fecha de consulta: 22.06.2010)
- VERA, Lamberto (2010), "Conceptos Básicos de Investigación y Estadística". (En línea) Disponible en: http://ponce.inter.edu/cai/reserva/lvera/CONCEPTOS_BASICOS.pdf
(Fecha de consulta: 23.06.2010)
- GRAJALES, Tevni, (2010), "Tipos de Investigación", (En línea) Disponible en: http://www.tgrajales.net/investipos.pdf (fecha de consulta: 23.06.2010).
- Vila Velasco, Paco. Directrices industriales de la seguridad y salud en el trabjo.www sicuris. com. (fecha de consulta: 23.04.2011).
- WIKIPEDIA, Enciclopedia Libre. (2010) "Muestreo en Estadística" (En línea) Disponible en: http://es.wikipedia.org/wiki/Muestreo_en_estad%C3%ADstica (fecha de consulta: 23.06.2010)
- ABRIL, Víctor Hugo (2010), "Proyectos UTA", (En línea) Disponible en: http://vhabril.wikispaces.com/PROYECTOS+UTA (fecha de consulta: 23.06.2010)
- WIKIBOOKS, (2010) "Tabulación de datos". (En línea) Disponible en: http://es.wikibooks.org/wiki/T%C3%A9cnicas_Estad%C3%ADsticas_para_las_Ciencias_de_la_Documentaci%C3%B3n/Descripci%C3%B3n/Tabulaci%C3%B3n (Fecha de consulta: 23.06.2010)
- WIKIPEDIA, (2010). "Estadística". (En línea) Disponible en: http://es.wikipedia.org/wiki/Distribuci%C3%B3n_t_de_Student (Fecha de consulta: 24.06.2010)
- WIKIPEDIA, (2010). "Cobit". (En línea) Disponible en: http://es.wikipedia.org/wiki/Cobit (Fecha de consulta: 24.06.2010)

ANEXOS

ANEXO 1

SRi.gov.ec

Desconectado

Búsqueda de Contribuyentes / *Información del Contribuyente*

Autorización de Documentos

Información del Contribuyente

Razón Social:	SERVICIO DE RENTAS INTERNAS
RUC:	1760013210001

Establecimiento Matriz

No. de Establecimiento	Nombre Comercial	Ubicación del Establecimiento	Estado del Establecimiento
037		PICHINCHA / QUITO / SALINAS N17-203 Y SANTIAGO	Abierto

Establecimientos Adicionales

No. de Establecimiento	Nombre Comercial	Ubicación del Establecimiento	Estado del Establecimiento
001		PICHINCHA / QUITO / PAEZ N22-53 Y RAMIREZ DAVALOS	Abierto
002		GUAYAS / GUAYAQUIL / AV. 10 DE AGOSTO 212 Y PEDRO CARBO Y PICHINCHA	Abierto
003		AZUAY / CUENCA / AV. REMIGO CRESPO 5-28 Y LORENZO PIEDRA	Abierto
004		MANABI / PORTOVIEJO / AV. UNIVERSITARIA 336 Y CESAR CHAVEZ ESQ.	Abierto
005		TUNGURAHUA / AMBATO / BOLIVAR 1560 Y LALAMA	Abierto
006		CHIMBORAZO / RIOBAMBA / PRIMERA CONSTITUYENTE Y EUGENIO ESPEJO	Abierto
007		BOLIVAR / GUARANDA / GARCIA MORENO S/N Y 7 DE MAYO	Abierto
008		CAÑAR / AZOGUES / BARTOLOME SERRANO 7-14 Y JULIO MARIA MATOVELLE	Abierto
009		CARCHI / TULCAN / AV. CORAL S/N Y VENEZUELA	Abierto
010		COTOPAXI / LATACUNGA / SANCHEZ DE ORELLANA 1568 Y PADRE SALCEDO	Abierto

ANEXO 2

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN AUDITORÍA GUBERNAMENTAL

CUESTIONARIO PARA ENCUESTA

Objetivo: Identificar el nivel de conocimiento del personal sobre las seguridades y controles establecidos en la Institución

Instrucciones: Lea detenidamente el texto de cada pregunta.

Marque con una X la alternativa de respuesta que usted elija

Si alguna pregunta considera no es clara, por favor solicite ayuda

Por favor no tachar, ni realizar enmendaduras

Preguntas:

1. ¿Conoce usted los controles implementados para la seguridad física de las instalaciones?

   Si ( )

   No ( )

2. ¿Ha sido instruido sobre las seguridades tecnológicas para el manejo de equipos de computación a su cargo?

   Si ( )

   No ( )

3. Identificando a la Seguridad Personal como las medidas que permiten minimizar riesgos o vulnerabilidades sobre su integridad física: ¿Considera usted que existen adecuadas seguridades personales en su lugar de trabajo?

   Si ( )

No ( )

4. ¿En caso de ausencia temporal de su lugar de trabajo, conoce las seguridades que debe aplicar?

   Si ( )

   No ( )

5. ¿Identifica claramente las áreas de acceso restringidos al público?

   Si ( )

   No ( )

6. ¿Considera usted adecuadas las seguridades para salvaguarda de la información que maneja?

   Si ( )

   No ( )

7. ¿En alguna ocasión ha perdido información física o magnética importante en el desarrollo de su trabajo?

   Si ( )

   No ( )

8. En caso de ser afirmativa la respuesta anterior: ¿Conocía el procedimiento a seguir para la recuperación de esta información?

   Si ( )

   No ( )

9. ¿En caso de siniestros, que se detallan a continuación, conoce el procedimiento a seguir?

Terremoto	Si	( )	Inundación	Si	( )
	No	( )		No	( )
Incendio	Si	( )	Erupción	Si	( )
	No	( )	Volcánica	No	( )

10. ¿Conoce los procedimientos a seguir para crear respaldos periódicos de la información que está bajo su responsabilidad?

    Si ( )

    No ( )

11. ¿Considera usted necesario implementar un adecuado programa de Seguridad Corporativa, que defina controles previos para minimizar los riesgos a los que estamos expuestos?

    Si ( )

    No ( )

Gracias por su valiosa colaboración

ANEXO 3

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN AUDITORÍA GUBERNAMENTAL

CUESTIONARIO PARA ENTREVISTA

Objetivo: Identificar la incidencia de las insuficientes seguridades y controles informáticos en los resultados de Auditoría Forense

Datos del Entrevistado:

Nombre: _____

Cargo: _____

Departamento: _____

Preguntas:

1. ¿Conoce usted si en el Servicio de Rentas Internas de Ambato se ha realizado un inventario de los riesgos a que están sujetos los bienes tangibles e intangibles?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

2. ¿En su departamento se han elaborado flujogramas de los procesos de control?

   Si ( )

No ( )

Explicación:_____
_____
_____
_____

3. En caso de ser afirmativa la respuesta anterior ¿Se han designado los responsables en cada uno de los procesos de control definidos?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

4. ¿Se ha definido un Plan de Socialización al personal a su cargo sobre la Seguridad Corporativa que aplica la entidad?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

5. En los casos de infracciones a las normas de seguridad implementadas, ¿se han definido y aplicado sanciones por incumplimiento?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

6. ¿Ha solicitado, al responsable del proceso de control, en caso de haberlo, informes de cumplimiento de las seguridades implementadas?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

7. ¿Dentro de las seguridades implementadas, considera usted que se cuentan con adecuadas técnicas de alerta temprana para detección de riesgos?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

8. ¿Considera usted que el nivel de cultura de seguridad que maneja el personal es adecuado?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

9. ¿Considera usted que los controles y seguridades físicas y tecnológicas actualmente en uso son suficientes y adecuados?

   Si ( )

   No ( )

   Explicación:_____
   _____
   _____
   _____

10. ¿Se han realizado evaluaciones sobre la incidencia de un adecuado Plan de Seguridad Corporativa sobre el número de delitos o infracciones cometidas por el personal?

    Si ( )

    No ( )

    Explicación:_____
    _____
    _____
    _____

Gracias por su valiosa colaboración