UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN GESTIÓN FINANCIERA

Tema: "LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA CONFIDENCIALIDAD EN UNIFINSA DE LA CIUDAD DE AMBATO"

Trabajo de Investigación

Previa a la obtención del Grado Académico de Magister en Gestión Financiera

AUTORA: Ing. Mariela Elizabeth López Argüello

DIRECTOR: Ing. Mg. Rubén Mauricio Sánchez Sánchez

Ambato – Ecuador

2013

Al Consejo de Posgrado de la Universidad Técnica de Ambato

El tribunal receptor de la defensa del trabajo de investigación con el tema: "**LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA CONFIDENCIALIDAD EN UNIFINSA DE LA CIUDAD DE AMBATO"**, presentado por la maestrante Ing. Mariela Elizabeth López Argüello, conformado por: Dr. Mg. Marco Antonio Espinoza Galora, Ing. Mg. Mario Cristóbal Rubio Sánchez, Ing. Dr. Ramiro Patricio Carvajal Larenas Miembros del Tribunal, Ing. Mg. Rubén Mauricio Sánchez Sánchez Director del trabajo de investigación y presidido por: Dr. Mg. Guido Hernán Tobar Vasco, Presidente del Tribunal; Ing. Mg. Juan Enrique 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.

Dr. Mg. Guido Hernán Tobar Vasco
Presidente del Tribunal de Defensa

Ing. Mg. Juan Enrique Garcés Chávez
DIRECTOR CEPOS

Ing. Mg. Rubén Mauricio Sánchez Sánchez
Director de Trabajo de Investigación

Dr. Mg. Marco Antonio Espinoza Galora
Miembro del Tribunal

Ing. Mg. Mario Cristóbal Rubio Sánchez
Miembro del Tribunal

Ing. Dr. Ramiro Patricio Carvajal Larenas
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 CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA CONFIDENCIALIDAD EN UNIFINSA DE LA CIUDAD DE AMBATO"**, corresponde exclusivamente a: Ing. Mariela Elizabeth López Argüello y de Ing. Mg. Rubén Mauricio Sánchez Sánchez Director del trabajo de investigación; y el patrimonio intelectual del mismo a la Universidad Técnica de Ambato.

---	---
Ing. Mariela Elizabeth López Argüello	Ing. Mg. Rubén Mauricio Sánchez Sánchez
Autora	Director

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este trabajo de investigación o parte de él 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.

Ing. Mariela Elizabeth López Argüello

DEDICATORIA

Este trabajo de investigación se lo dedico a mis padres por ser quienes me inculcaron los valores que me han permitido ser una persona íntegra, a mi sobrina Paola, quien pudo apoyarme incondicionalmente. A Dios por brindarme cada minuto de vida, a mis amigos quienes con sus consejos me motivaron a seguir adelante con mis estudios.

Ing. Mariela Elizabeth López Argüello

AGRADECIMIENTO

Mi sincero agradecimiento a la Universidad Técnica de Ambato y al Centro de Posgrado de la Facultad de Contabilidad y Auditoría por permitirme crecer en conocimientos, a mi querida Institución por haberme apoyado tan de cerca en el desarrollo de este trabajo investigativo, como no agradecer al Ing. Mg. Mauricio Sánchez, quien con su paciencia supo guiarme durante todo el proceso.

Ing. Mariela Elizabeth López Argüello

ÍNDICE GENERAL DE CONTENIDOS

CONTENIDO **PAG.**

ÍNDICE DE TABLAS

Nro. CONTENIDO PAG.

ÍNDICE DE GRÁFICOS

Nro. CONTENIDO PAG.

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN GESTIÓN FINANCIERA

LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA CONFIDENCIALIDAD EN UNIFINSA DE LA CIUDAD DE AMBATO

Autor: Ing. Mariela Elizabeth López Argüello
Tutor: Ing. Mg. Rubén Mauricio Sánchez Sánchez
Fecha: 05 de Enero de 2013

RESUMEN

En la actualidad, la información se ha convertido en uno de los activos más importantes para las empresas, y por lo tanto, debe ser protegida de un sin número de amenazas. La confidencialidad de la información es un tema que realmente preocupa a todos los sectores, financieros, públicos, estado, vaticano etc, ya que en algún momento han sido víctimas de fugas de información. La confidencialidad es un gran reto para las instituciones ya que con las innovaciones tecnológicas es más difícil definir límites geográficos del ámbito de utilización y protección de la información. Estar conscientes y determinar qué debe ser protegido, por qué, de qué debe ser protegido, y como protegerlo, va a permitir reaccionar con rapidez ante cualquier incidente de seguridad de la información relacionado con la confidencialidad. Un aspecto fundamental es la cultura en seguridad de la información que poseen los colaboradores dentro de una organización, sumado a las herramientas tecnológicas creadas para controlar fugas de información ayudan a mitigar y a evitar consecuencias desfavorables para las empresas.

Descriptores: Cultura en seguridad de la información, confidencialidad, fuga de información, activo de información, plan de tratamiento de riesgo.

TECHNICAL UNIVERSITY OF AMBATO

POSTDEGREE STUDY CENTER

MASTER IN FINANCIAL MANAGEMENT

CULTURE IN INFORMATION SECURITY AND ITS RELATIONSHIP WITH THE CONFIDENTIALITY IN UNIFINSA AMBATO

Author: Ing. Mariela Elizabeth López Argüello
Tutor: Ing. Mg. Rubén Mauricio Sánchez Sánchez
Date: January 05, 2013

SUMMARY

Today, information has become one of the most important assets for companies, and that's why it must be protected of a number of threats. Confidentiality of information is an issue that really concerns all sectors, financial, public, state, Vatican etc. Because at some point have suffered leaks. Confidentiality is a major challenge for the institutions and technological innovations that are more difficult to define geographic boundaries of the field of use and protection of information. Be aware and determined to be protected, why, what should be protected, and how to protect it, will allow fast response to any security incident related information confidential. A key aspect is the safety culture of the information held by employees in an organization coupled with technological tools created to control information leakage help mitigate and prevent adverse consequences for businesses.

Descriptor: Culture in information security, confidentiality, data leakage, information asset, risk treatment plan.

INTRODUCCIÓN

El presente trabajo de investigación se elaboró tomando en cuenta la importancia de la preservación de la confidencialidad de la información, la información se ha convertido en uno de los activos más críticos en las empresas y hay que protegerla.

Hay que estar conscientes que ningún sistema es 100% seguro, por lo tanto, cualquier medida que se adopte es importante debido a que se dificulta el acceso de terceros a información confidencial.

El presente trabajo de investigación tiene como objetivo, contar con un plan de tratamiento de riesgo, donde se identifiquen controles y acciones preventivas, que mitiguen los riesgos asociados a la fuga de la información, la entidad a estudiar es la Sociedad Financiera Unifinsa.

En el capítulo I, se presenta el problema de investigación dando una breve descripción de la fuga de información en su aspecto: Macro, Meso y Micro, análisis crítico, prognosis y objetivos.

En el capítulo II, se realiza un estudio conceptual en donde abarca información bibliográfica, base legal y términos básicos a utilizarse en el tema de estudio.

En el capítulo III, se describe como se llevó a cabo la investigación señalando los métodos y técnicas que se aplicarán, así mismo la población a estudiarse, planteamiento de la hipótesis y sus variables.

En el capítulo IV, se realizó un amplio estudio basándose en las observaciones de campo pudiendo así comprobar la hipótesis.

En el capítulo V, se evidenció las conclusiones y recomendaciones de la investigación realizada.

Finalmente, en el capítulo VI, se desarrolló en su totalidad la propuesta planteada, el cual mitiga y controlar el problema mediante un plan de tratamiento de riesgo.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Tema de Investigación

"La cultura en seguridad de la información y su relación con la confidencialidad en Unifinsa de la ciudad de Ambato"

1.2. Planteamiento del Problema

1.2.1. Contextualización

1.2.1.1. Contexto macro

La fuga de información es lo que ocurre cuando algún dato o activo de información que tenga valor para una organización, pasa a manos ajenas, perdiendo la cualidad de confidencialidad que le fue asignada.

La empresa **ESET (2012: Internet)** una compañía global de soluciones de seguridad, fundada en 1992 y con oficinas centrales en Bratislava, Eslovaquia, y de Coordinación en San Diego, Estados Unidos de Norte América; Buenos Aires, Argentina y Singapur, publicó un artículo titulado "Alerta: Fuga de Información de Tarjetas de Crédito.

En las últimas horas, las prestigiosas empresas VISA y MasterCard han emitido un alerta a las entidades bancarias sobre una posible fuga de información en un sistema de procesamiento de pago de tarjetas de

crédito en Estados Unidos. Fuentes del sector financiero han catalogado a este suceso como de carácter masivo, y pueden estar involucrados más de 10 millones de números de tarjetas.

Esta situación comenzó la semana pasada con el envío de alertas por parte de las mencionadas empresas informando sobre casos particulares de tarjetas de crédito comprometidas. Distintas asociaciones vinculadas a este rubro aseguran que el compromiso del mencionado sistema de procesamiento ocurrió posiblemente entre el 21 de Enero y el 25 de Febrero del 2012. Cabe aclarar que un vocero de MasterCard aclaró que sus sistemas no fueron vulnerados y que la compañía está alertando a las entidades bancarias sobre las posibles cuentas que fueron comprometidas.

Tanto VISA como MasterCard no aseguraron cual es la entidad de procesamiento de pagos que fue vulnerada y dio origen a este tipo de fuga. Sin embargo, las entidades bancarias comenzaron una investigación sobre las transacciones en aquellas tarjetas que fueron comprometidas con la finalidad de poder detectar algún tipo de patrón en las operaciones.

Aún no está claro cómo se produjo esta fuga de información en el sistema de procesamiento, sin embargo ya existen algunas hipótesis. De esta manera, el proveedor de servicios financieros online PSCU (*Public Service Credit Union* por sus siglas en inglés), afirmó que envió un alerta a 482 cooperativas financieras (*credit unions*) que al parecer poseen tarjetas que fueron afectadas por la fuga, llegando a un total de 56.455 cuentas de VISA y MasterCard comprometidas.

Además el mencionado proveedor de servicios afirmó que solamente un número menor de ese grupo de tarjetas, tan solo 876 cuentas, se les detectó actividad fraudulenta.

Finalmente, MasterCard aseguró que tomará medidas para mantener resguardada la información de las cuentas y continuará con el proceso de monitorización."

Otro de los casos de Fuga de Información fue el artículo publicado por Diario El Universo (2012: Internet), titulado "Advertencia de despidos por fuga de información".

Con la finalidad de evitar inconvenientes al personal de la EP Petroecuador por la fuga y mal uso de la documentación e información generada y utilizada en las actividades de nuestra empresa, se recuerda a todo el personal que tienen que dar cumplimiento irrestricto de los artículos 175, 176 y 178 de la normativa de Gestión aprobada (...)" el 7 de abril del 2010.

Con este párrafo inicia el memorando Nº 00043-PGER-DGER-DTIC-APL-2012, elaborado el 18 de enero pasado y difundido en la empresa y en el Instituto de Estudios Petroleros el 30 y el 31 de enero. El documento está suscrito por el gerente general de la estatal petrolera, Marco Calvopiña.

La desobediencia a tal disposición "será considerada como falta grave y constituirá causal suficiente para dar por terminado el contrato individual de trabajo de un obrero o el nombramiento de un servidor público", añade.

Las dos hojas membretadas con el asunto: Mal uso de la información y documentación detallan además los tres artículos que los empleados y obreros de la petrolera pública deberán cumplir so pena de perder sus puestos de trabajo.

El artículo 175 de la norma de Gestión se refiere a que "los servidores públicos y obreros de Petroecuador deben tener presente que los documentos de cualquier naturaleza, así como los valores en efectivo,

divisas, cheques, documentos, informes, cartas, información técnica, reportes, estadísticas, registros sísmicos, procedimientos industriales, operativos y tecnológicos, roles de pago, expedientes personales, entre otros, manejados por ellos, son de interés propios de la empresa y de terceras personas, confiados a su pericia y diligencia".

Por ese considerando, la empresa "exige" la reserva y confidencialidad de toda la información manejada por ellos.

Además, no podrán efectuar declaraciones a los medios de comunicación o publicar en internet asuntos relacionados con la actividad de la empresa "sin contar con la autorización por escrito del gerente general o respectivo gerente de la Unidad de Negocios".

De ese modo se busca evitar que las personas ajenas a Petroecuador accedan a información confidencial, así como prohibir a los servidores públicos que "negocie con terceras personas información confidencial o estratégica".

El incumplimiento de esa disposición interna, fuera de ser sancionado con el despido, acarreará también responsabilidades administrativas, civiles y penales hacia el infractor.

En el memorándum se prohíbe también que las denuncias de las irregularidades puedan hacerse públicas. "En caso de que un servidor público u obrero tenga conocimiento cierto de que existe una razonable posibilidad, de que haya ocurrido o esté ocurriendo alguna irregularidad, deberá reportarla inmediata y confidencialmente en forma verbal o escrita, a su superior".

Disposiciones: Petrolera estatal Confidencial

Las disposiciones dadas en el oficio elaborado el 18 de enero están sujetas en la resolución P2010001 del 7 de abril del 2010, relacionada con la confidencialidad, entrega de información y denuncias de irregularidades dentro de la empresa.

Hay que destacar que la Fuga de Información no es un tema nuevo para la industria de la seguridad de la información, solo que hoy en día parece ser difícil evitarlo en las mesas de discusión sobre la privacidad y la confidencialidad en las empresas y por qué no decirlo también en el ámbito personal.

1.2.1.2. Contexto meso

No cabe duda de que el fenómeno Wikileaks determinó un antes y un después en cuanto a lo que se refiere a fuga de información, no porque antes no ocurriera, sino porque en la mayoría de las ocasiones las fugas no se hacen públicas para salvaguardar la imagen de las empresas e instituciones hacia afuera, y aquí es donde el caso marcó un límite. Sin hacer un juicio de valores sobre el caso, es posible entender que la trama del asunto no es en última instancia la información en sí que se haya filtrado, sino más bien la posibilidad de que tal cosa pueda sucederle a organizaciones tan grandes y preparadas, lo que deja en claro que podría ocurrirle también a empresas y organizaciones más pequeñas.

Si bien lo normal no es que una persona desee robar información intencionalmente, no se puede negar que la posibilidad exista. Lo que sí es posible afirmar es que cualquiera que esté involucrado en la fuga intencional de información pertenecerá al grupo de empleados disconformes con la empresa, o que se hayan visto perjudicados por la misma, situación que es conveniente que intente conocer para evitar

permanecer desprevenidos. Esto sin contar el espionaje interno que puede existir por parte de empleados que lo realizan en función de intereses externos, perjudicando a la propia organización a la que pertenecen.

De todos modos, esto no implica que la fuga pueda darse solo por malas intenciones del propio empleado, ya que en muchos casos un atacante intenta conseguir información utilizando técnicas de Ingeniería Social, buscando engañar al usuario. De esta manera, los usuarios simplemente pueden ser víctimas de algún fraude o engaño que podrían dejar expuesta a la empresa por impericia. Además, algo tan simple como una infección de malware transportado en un pendrive podría introducir un riesgo importante en una empresa si no cuenta con un sistema que pueda prevenirlo de manera eficiente.

Si bien resulta difícil que ciertos problemas sean mitigados en su totalidad, es posible estudiarlos desde distintos ángulos a fin de que puedan reducirse las posibilidades de ocurrencia y se disminuyan los riesgos.

1.2.1.3. Contexto micro

La presente investigación se realizó en una Sociedad Financiera, de la Ciudad de Ambato, Institución Financiera de gran prestigio, que tiene 18 años sirviendo a la comunidad, se ha convertido en una de las mejores Sociedades Financieras del Ecuador.

Es la primera Institución Financiera, controlada por la Superintendencia de Bancos y Seguros, en obtener la certificación ISO 9001-2000 (*International Standard Organization* por sus siglas en inglés) a todos los procesos integrados de la Organización.

“La seguridad es una cadena que siempre se rompe por el eslabón más débil”.

Actualmente, los usuarios toman demasiado a la ligera la responsabilidad que implica el manejo correcto de la información.

Uno de los tipos más comunes de fuga de información es la fuga de contraseñas, las contraseñas siguen siendo un punto débil de los usuarios.

Una misma contraseña, que es utilizada para varios servicios, puede compararse con una persona que usa la misma llave para su casa, oficina, caja fuerte, bodega. El problema radica, si un código malicioso roba esa credencial de acceso, o un atacante obtiene la misma mediante fuerza bruta, tendrá acceso total a varios servicios incluyendo redes sociales, correo electrónico, bancos, etc. Lo cual representa un serio riesgo para la seguridad de la información.

Otro aspecto preocupante es, que los usuarios aseguran utilizar una palabra o frase real como parte de la contraseña. Aunque esto facilita que la misma sea recordada fácilmente, también permite que sea vulnerada e incluso adivinada en menor tiempo y utilizando pocos recursos. En base a la misma interrogante, es común emplear datos personales como números de documento, fechas de nacimiento, entre otras cosas, para formar una clave, lo que representa otro problema más para la seguridad. Un atacante con conocimientos mínimos sobre su potencial víctima podría tener una mayor posibilidad de éxito si este tipo de información es utilizada para formar credenciales de acceso. Hay usuarios que utilizan combinaciones aleatorias para formar contraseñas, este método aunque es más seguro si se implementa correctamente, podría no serlo si el usuario al encontrarse frente a la dificultad de recordarla, anota la clave en un documento o papel.

La Institución cuenta con políticas de seguridad de la información, pero las mismas no son monitoreadas de forma adecuada, ya que no se cuenta con el personal necesario para realizar estas funciones.

1.2.2. Análisis crítico

La fuga de Información es un problema que aqueja a muchas organizaciones no importa su naturaleza o si es grande o pequeña, en algunas ocasiones tienen su origen en usuario internos con acceso autorizado a la información. Las motivaciones de estos empleados para apoderarse de dicha información corporativa se asocian a menudo con la situación de crisis económica actual, al aumentar el número de despidos, los trabajadores que temen por su futuro en la corporación deciden disponer de la información confidencial para posicionarse mejor en el mercado de trabajo. El despecho y/o conseguir un dinero “extra” a través de la venta de dicha información al mejor postor son otras de las posibles motivaciones para cometer este delito de fuga de datos confidenciales.

El problema radica en la dificultad de administrar y gestionar la enorme cantidad de datos que procesan las organizaciones, en este sentido, teniendo en cuenta que cada nivel de usuarios deberá acceder a distintos archivos y datos, y que estos además viajarán por las redes y se almacenarán en distintas ubicaciones dentro y fuera del centro de cómputo.

El tema no puede ser encarado desde una sola perspectiva o área de una organización, sino que requiere de una tarea conjunta entre distintas áreas y personas, y un completo apoyo de parte de la administración correspondiente, dado que estamos hablando de riesgos, y el riesgo es algo que por definición misma no es posible eliminar solo reducir.

En el año 2011, se realizó, una revisión del comportamiento de los empleados frente a la seguridad de la información y, se ha detectado que el 40% de los empleados de Unifinsa, deja desprotegido su equipo de cómputo, especialmente en las horas que el personal se retira a su lunch.

Este es uno de los escenarios, donde usuarios mal intencionados pueden aprovechar y obtener información sin autorización del propietario.

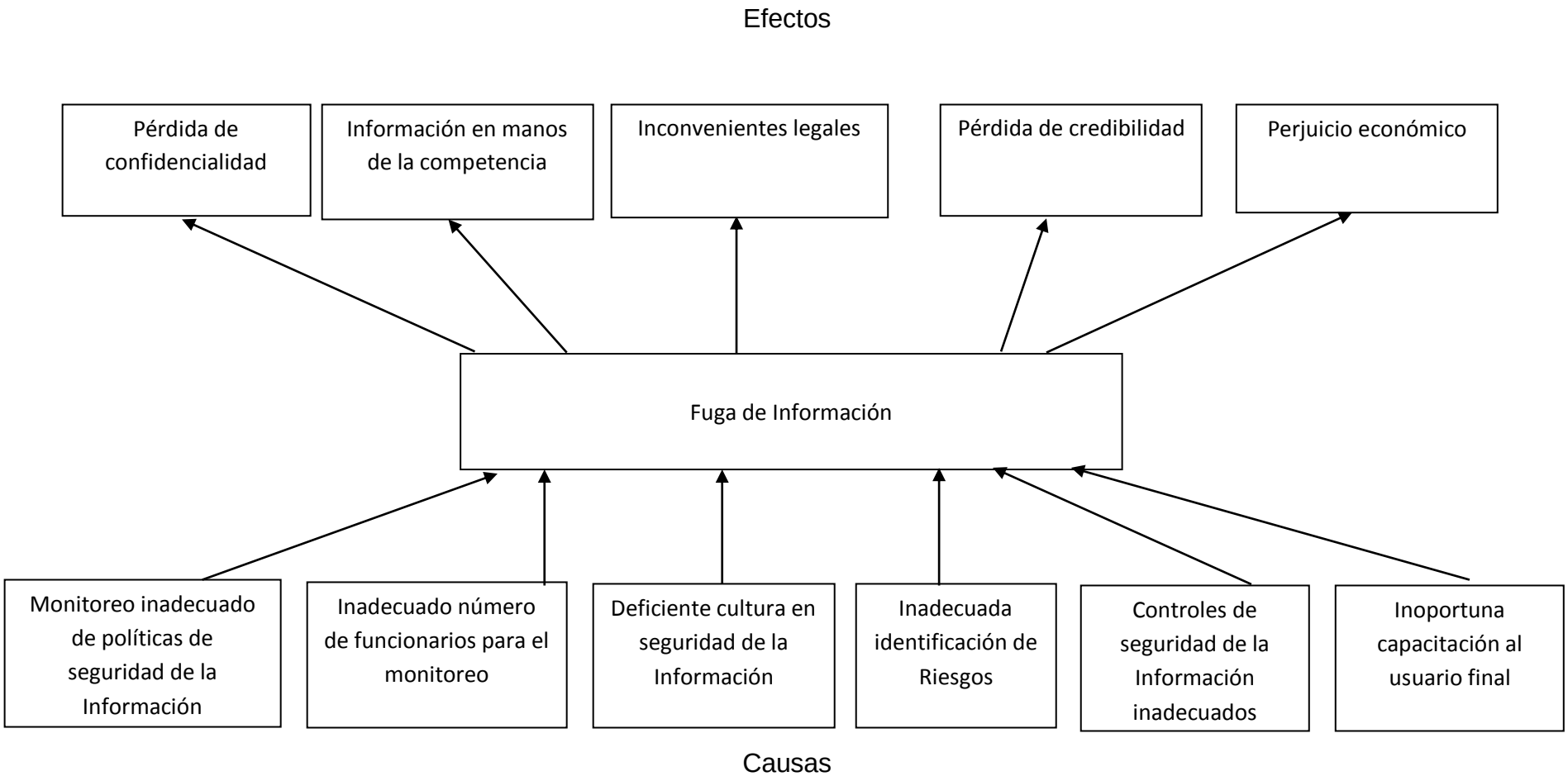
Adicionalmente una de las principales herramientas que contribuyen a la fuga de información es el uso de impresoras y copiadoras sin ningún control.

El 80% de los colaboradores poseen libre acceso a impresoras y copiadoras.

De una muestra de 100 documentos (reportes impresos), encontrados en un el basurero de un colaborador, el 10% contenía información confidencial como nombres de clientes, direcciones y teléfonos. Esto evidencia que no existe un adecuado tratamiento de la información (documentos en papel), al momento de desecharla.

Existen varios escenarios que pueden provocar fuga de información intencional o no intencional, por este motivo se tomaron acciones proactivas en lugar de actuar de manera reactiva, y para esto se procedió a realizar la identificación de la información que tiene impacto para la organización, una evaluación de riesgo, es decir identificar como es la relación de amenazas y vulnerabilidades, con esta información se identificó ¿Qué acciones se deberían tomar para mitigar el riesgo?, ¿Qué riesgo se acepta, se transfiere y se evita?, hasta la definición de lo que también es conocido como plan de tratamiento del riesgo.

1.2.2.1. Árbol de problemas



1.2.2.2. Relación causa-efecto

La pérdida de confidencialidad, se origina debido a la deficiente cultura en seguridad de la información.

1.2.3. Prognosis

La fuga de información puede ser un inconveniente muy grave para una empresa ya que al parecer todo el mundo sabe que existe pero nadie le hace frente.

Si en una organización no se cuenta con una cultura adecuada en seguridad de la información, control y administración de riesgos por más efectivos que sean sus procesos y su tecnología jamás funcionarán acorde ya que no se encuentran dentro de un lineamiento corporativo.

El gran problema de la fuga de información es que podría convertirse en un negocio, llegando a perjudicar a la institución. La pérdida de valores, falta de ética, de moral puede llevar a una persona a sustraer información para comercializarla.

En el internet es cada vez más común encontrar avisos clasificados donde se comercializan datos e información, como por ejemplo, vendo una base de datos y, efectivamente se realizan las transacciones donde hay intermediarios y explícitamente se prestan cuentas bancarias para realizar los correspondientes pagos. En efecto, se compran las bases de datos con información confidencial tanto a nivel personal como información sensible de organizaciones y empresas, las cuales son de carácter reservado.

Hoy en día estamos en un mundo donde no existen fronteras, la información se maneja en cualquier país y a través de dispositivos

móviles de todo tipo. Entonces, la información está en todas partes y es muy difícil detectar los hechos que rodean su fuga.

1.2.4. Formulación del problema

¿Es la deficiente cultura en seguridad de la información la principal causa de la fuga de información, lo que conlleva a una pérdida de confidencialidad, en Unifinsa de la ciudad de Ambato?

1.2.5. Preguntas directrices

¿Qué impacto tendría Unifinsa, en el caso que información confidencial, llegara a parar en manos de la competencia?

¿Por qué es importante una adecuada identificación de riesgos?

¿Cómo aportaría mejorar los controles de seguridad de la información?

¿Cómo ayudan las políticas de seguridad de la información a reducir la fuga de información?

¿Por qué una fuga de información, puede causar un perjuicio económico para Unifinsa?

¿Por qué la capacitación oportuna al usuario final, puede reducir la fuga de información?

¿Por qué la fuga de información podría causar inconvenientes legales?

¿Se cuenta con un número adecuado de funcionarios responsables de controlar y monitorear la fuga de información?

1.2.6. Delimitación

- **Campo:** Gestión Financiera
- **Área:** Riesgo Operativo
- **Aspecto:** Fuga de Información
- **Temporal:** El tiempo del problema es el año 2011
- **Espacial:** Esta investigación se realizará en Unifinsa, que se encuentra ubicado en la Av. Cevallos y Mera de la ciudad de Ambato, de la provincia de Tungurahua. (ver RUC en Anexo 1).

1.3. Justificación

La fuga de información se asocia con tres elementos que son personas, procedimientos y tecnología, y aunque todos están unidos e interactúan de forma coordinada, la fuga de información se da primariamente por personas, impactando los procedimientos y la tecnología.

Es importante tener en cuenta, como toda la información que va alrededor de la empresa y lo que la hace exitosa dentro del ambiente de negocios, cada vez las organizaciones están empoderando a la gente sobre el manejo de la información para optimizar y mejorar. En otras palabras, se le ha dado más protagonismo a la información y, por supuesto, a la tecnología como herramienta de desarrollo.

La evolución y el crecimiento es innegable, pero, en los asuntos de manejo de información, no se sabe qué es lo importante ni lo confidencial, ni qué lo público. No se ha avanzado en la cultura de saber qué es lo realmente crítico para la organización.

Otros estudios muestran estadísticas sobre la fuga de información y señalan que cerca del 80% de los eventos relacionados con la

información son producidos por motivaciones sin intención, por no conocer qué pasa; por ignorancia o por aprovechamiento de otras personas que simplemente desconocen el funcionamiento y la importancia de la información, y permiten la fuga de la misma.

La información es un activo esencial para los negocios de la empresa y consecuentemente necesita cuidado y protección.

La cultura en seguridad de la información es una responsabilidad de Unifinsa, por lo tanto debe aplicar a todos los funcionarios y empleados que utilizan la información, que supervisan a usuarios que manejan información que administran, respaldan o dan mantenimiento a sistemas de información.

Por este motivo es importante entender que la seguridad de la información no solo depende de equipos informáticos sino también de personas.

Este trabajo se elaboró con el fin de identificar de manera objetiva que activos de información se requiere proteger, de qué debe ser protegido y como protegerlo, con el fin de evitar fugas de información que pueden tener un alto impacto en la confidencialidad en Unifinsa.

1.4. Objetivos

1.4.1. Objetivo general

Estudiar la relación de la cultura en seguridad de la información con la pérdida de confidencialidad, en Unifinsa de la ciudad de Ambato, para el control de la fuga de información.

1.4.2. Objetivos específicos

Evaluar el grado de cultura en seguridad de la información del personal de Unifinsa de la ciudad de Ambato para la determinación de falencias.

Establecer los medios de pérdidas de confidencialidad que presenta Unifinsa de la ciudad de Ambato para la determinación del impacto en la organización.

Proponer la implementación de un plan de tratamiento de riesgo que contribuya al control de la fuga de información en Unifinsa.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes Investigativos

La fuga de información no es una problemática nueva para la industria de la seguridad de la información ya que a menudo ocurren casos que aquejan a las organizaciones, aunque también puede afectar a cualquier individuo en su ámbito personal. La fuga de información puede ser un inconveniente muy grave para una empresa en caso de no implementar controles para que no suceda. Además, se deben tener en cuenta medidas en el caso desafortunado que así ocurra.

En la tesis de **José Luis Rojas y Juan José Vela (2011: Internet)**, señala que, la seguridad de la información tiene muchas falencias ya que no se le ha dado la importancia. Para muchas empresas al igual que lo que se ha visto en la evaluación realizada a Fabril Fame S.A, la seguridad de la información está ligada a realizar respaldos de la información y mantenerlos seguros; sin darse cuenta que en realidad existen muchos puntos adicionales los cuales necesitan ser revisados ya que generan infinidad de riesgos y pueden llegar a ocasionar problemas graves para la organización sino se implementa los respectivos controles.

En la tesis de **Carlos Xavier Haro (2011: Internet)**, comenta que, Una aplicación de mensajería electrónica puede ser utilizada para la fuga de información confidencial. A diferencia del correo electrónico, donde se pueden aplicar mecanismos para identificar posibles pérdidas, es muy

difícil llegar a identificar cualquier fuga que se realice a través de una conexión de este tipo.

Los datos e información que fluye dentro y fuera de una organización o empresa, constituye un activo muy importante de la misma, es por ello que se debe poner especial atención con respecto a su seguridad y como mantener esa información a buen recaudo.

Se hace necesario entonces la creación de políticas de seguridad de información propias de la organización que incluyan normas, procedimientos, estrategias y sugerencias que los usuarios de dicha organización deberán tomar en cuenta para no ser víctimas de ataques voluntarios o involuntarios que puedan darse a la información de esa organización o empresa.

La mensajería instantánea (MI) se ha convertido en una herramienta informática esencial en el hogar y los negocios. Le permite evitar costos de larga distancia en los que incurriría si hablara por teléfono y le permite saber inmediatamente si la persona que está tratando de contactar está en la computadora. Puesto que usted se comunica en tiempo real, intercambiar mensajes con las personas a través de la Mensajería Instantánea (MI) es tan simple como escribir un texto en la computadora y oprimir la tecla Enter.

Tomando como referencia a **Deloitte (2008: Internet)**, que es una firma bajo la cual decenas de miles de dedicados profesionales colaboran alrededor del mundo para proporcionar de auditoría, consultoría, asesoramiento financiero, gestión de riesgos, y los impuestos de servicios a los clientes seleccionados. Publicó un artículo titulado “La "Amenaza Fantasma”, donde se menciona:

“Fuga de Información se ha convertido en la frase de moda para describir los incidentes de seguridad de información ocurridos durante los últimos años. Aunque el término puede ser interpretado de diversas formas y usado en variedad de contextos, estamos de acuerdo que causa una reacción universal: miedo. Aun cuando es difícil dimensionar el daño de las fugas de información, no hay duda que la exposición de las bases de datos, o robos de información en computadores, entre otros, afectan y/o disminuyen la confianza de los clientes, con las respectivas consecuencias negativas para la organización.

El aumento de la recolección y almacenamiento de datos por organizaciones de todas las industrias y sectores, acompañado del incremento de sofisticadas tácticas de hackeo informático para robar información sensitiva, y de la poca, y a veces nula, conciencia dentro de la propia organización, las ha forzado a reconocer y enfrentar directamente esta amenaza que dejó de ser fantasma.

En este escenario, las organizaciones están expandiendo el proceso de investigación de antecedentes para clientes, empleados o contratistas.

Verificar credenciales educacionales, experiencia laboral y certificaciones profesionales, son aspectos que ayudan a tener un diagnóstico sobre la honestidad del postulante. Adicionalmente, el sector público y privado está requiriendo a los postulantes ser sometidos a chequeos de antecedentes judiciales o penales. Sin embargo, es necesario destacar que antes de implementar un proceso de este tipo, se debe determinar si estos controles están dentro de la legalidad. Asimismo, es prudente considerar en este chequeo al personal que actualmente está trabajando en la organización, especialmente a aquellos empleados con acceso a información sensitiva, pero también puede incluirse a contratistas, empleados temporales, personal de mantenimiento y estudiantes en

práctica, e incluso a proveedores, a quienes se les exige antecedentes financieros y laborales.

En definitiva, una verificación de antecedentes más exhaustiva ayuda a salvaguardar la información de la empresa.
Desde una perspectiva de control, los auditores internos están en una muy buena posición para evaluar si sus organizaciones tienen bien identificados los diferentes medios o dispositivos de almacenamiento de datos; analizar los riesgos de privacidad asociados con estos tipos de medios; e implementar los controles necesarios para mitigar cualquier vulnerabilidad. En este sentido, las bases de datos, notebooks y correspondencia por e-mail presentan desafíos únicos para los encargados de seguridad en cuanto a la confidencialidad.

En lo que se refiere a las bases de datos, el volumen y la naturaleza sensible de la información que contienen las convierten en un preciado blanco de agentes internos y externos no autorizados, que tienen gran interés acceder a esta información.

En lo que se refiere a los Notebooks, es importante que estos equipos sean anclados a los muebles o provistos de métodos de encriptación para salvaguardar la información en caso de robos o extravío. Los auditores internos deben realizar inspecciones sorpresa en terreno para verificar si estos dispositivos están configurados y si los empleados conocen y saben utilizar los protocolos de seguridad. Demás está decir que estas técnicas de nada sirven si los empleados no mantienen adecuadamente las contraseñas con que acceden remotamente a la red de su organización o a su propio notebook.

Respecto del e-mail, es necesario establecer mecanismos para prohibir el envío de información confidencial por esta vía, o implementar controles preventivos. Como ejemplo, hay organizaciones en las que, antes de

enviar un mensaje, el emisor debe proveer de una clave al receptor para que éste pueda ver la información enviada. Con software muy simple, los auditores pueden detectar a empleados que envían información confidencial sin usar este control de acceso y bloquear su cuenta de e-mail. Nuevamente, este tipo de revisiones debe estar bajo el resguardo de las normativas y leyes vigentes.

Finalmente, aunque ninguna organización es inmune a la fuga de información, los auditores internos pueden minimizar los riesgos implementando los adecuados mecanismos de prevención. Las organizaciones exitosas actúan en forma preventiva para proteger datos sensitivos, implementando un conjunto de medidas para educar a los empleados, identificar vulnerabilidades y detectar el uso indebido de la información. Adecuadas políticas de información, continuas evaluaciones de riesgos, capacitación en seguridad, chequeo de los anteriores trabajos de los empleados, monitoreo sobre obligaciones de cumplimiento normativo y una disciplinada estructura de estándares a cumplir, son los componentes centrales de una efectiva estrategia de seguridad."

Según **Andrés Velázquez, (2012: Internet),** presidente y fundador de Mattica, compañía dedicada a las investigaciones digitales, en un artículo titulado "Delitos informáticos causan pérdidas millonarias en bancos y empresas", indica:

Si bien los bancos normalmente tienen un fuerte enfoque en seguridad, no están exentos de sufrir ataques maliciosos o algún robo de información interna por un empleado descontento o un ejecutivo que se va a la competencia. Las pérdidas que esto genera pueden ser grandes en términos económicos, pero son exponenciales en lo que se refiere a la confianza de sus clientes.

En la tesis de **Manolo Roberto Fabara Villacís (2007: Internet)**, menciona que, mediante el estudio tanto de la gestión de la información y conocimiento como el de la gestión de la seguridad de la información ha permitido generar una metodología que permite a las empresas e industrias según sus recursos y capacidades establecer los pasos necesarios para poder escalar en la metodología generada y así como resultado tener un grado de seguridad aceptable de su información y conocimiento.

La gestión del conocimiento y de la información es un paso fundamental para el mejoramiento de una institución ya que mediante este proceso además de conocer el valor real de los recursos y capital intelectual de la organización nos da una visión más clara de las debilidades o falta de conocimiento e información que tiene la institución además concede a dicha empresa una ventaja estratégica respecto de sus iguales.

La gestión de riesgos permite disminuir la incertidumbre con lo cual se da una sensación de confianza tanto al interior como al exterior de la empresa.

La gestión de riesgos permite prepararnos ante cualquier amenaza y disminuir las debilidades de la empresa.

La gestión de seguridad de la información en las instituciones no es un producto si no un proceso.

La gestión de seguridad depende de todos los usuarios de la información y no tan solo del área informática.

La gestión de seguridad de la Información se ayuda de metodologías y técnicas complementarias como son: La gestión de la información y conocimiento, gestión de riesgos, modelo magerit (metodología de

análisis y gestión de riesgos de los sistemas de información), Norma ISO 17799 (*International Standard Organization* por sus siglas en inglés), que permiten de forma coordinada generar un status adecuado de seguridad en la organización.

Las leyes que rigen en nuestro país no son lo suficientemente adecuadas para la protección de la información.

Para determinar el nivel adecuado de seguridad para la institución principalmente debemos observar el tipo de información que queremos asegurar.

Para un mínimo nivel de seguridad como el necesario en las micro empresas del Ecuador, es tan solo necesario subir hasta el primer escalón de la metodología de gestión de seguridad de la información.

Tanto las pequeñas y medianas empresas deben subir hasta el segundo escalón de implementación de la metodología de gestión de seguridad de la información para tener un nivel de seguridad adecuado para ellas"

2.2. Fundamentación Filosófica

La presente investigación se encontró ubicada en el paradigma crítico propositivo; crítico porque analizó una realidad cultural; y propositivo por cuanto buscó plantear una alternativa de solución con el fin de contribuir al mejoramiento de las condiciones actuales de la seguridad de la información permitiendo conocer el problema tanto teórico como práctico, y así pudo llegar a cualificar y cuantificar las causas y efectos del mismo.

2.3. Fundamentación Legal

Registro Oficial 545 (RC2)
29 septiembre 2011
Libro I
Normas Generales Para la Aplicación de la ley
General de Instituciones del Sistema Financiero
Título X
De la Gestión y Administración de Riesgos
Capítulo V
De la Gestión del Riesgo Operativo
resolución No JB-2005-834 de 20 de octubre del 2005

Sección I.- Ámbito, definiciones y alcance

Artículo 2

2.2 Evento de riesgo operativo.- Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

2.3 Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos;

2.4 Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

2.5 Insumo.- Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

2.6 Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

2.7 Actividad.- Es el conjunto de tareas;

2.8 Tarea.- Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y mesurable;

2.9 Procedimiento.- Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

2.11 Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

2.12 Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones;

2.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

2.14 Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

2.15 Tecnología de información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la

información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

2.18 Responsable de la información.- Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones;

2.19 Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

2.20 Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

2.21 Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información prestablecida;

2.22 Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

2.23 Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

2.25 Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

2.26 Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

2.27 Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

2.35 Riesgo legal.- Es la probabilidad de que una institución del sistema financiero sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas. (Sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

De acuerdo con lo dispuesto en el numeral 2 del artículo 18 del Código Civil, los términos utilizados en la definición de riesgo legal se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras, a menos de que tengan definiciones diferentes expresadas en la ley, reglamentos y demás normativa. (Incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Artículo 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.
El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.35 del artículo 2.

El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

Sección II.- Factores del riesgo operativo

Artículo 4.-

4.2.3 Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.

Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

4.3 Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información. Dichas políticas, procesos y procedimientos se referirán a:

4.3.1 Con el objeto de garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;

4.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;

4.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;

4.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;

4.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,

4.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

4.3.2 Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;

4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

4.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,

4.3.4 Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

4.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;

4.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;

4.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;

4.3.4.4 Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;

4.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

4.3.4.6 Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

4.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;

4.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;

Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;

4.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,

4.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

4.3.2 Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;

4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

4.3.3 Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,

4.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

4.3.4 Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

4.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes

relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;

4.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;

4.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;

4.3.4.4 Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;

4.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

4.3.4.6 Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

4.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;

4.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;

4.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;

4.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;

4.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,

4.3.4.12 Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

4.3.5 Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

4.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;

4.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;

4.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,

4.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

4.3.6 Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

4.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;

4.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;

4.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,

4.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

4.3.7 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada, las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

4.4 Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

Sección III.- Administración del riesgo operativo

Artículo 10.- Una vez identificados los eventos de riesgo operativo y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la institución, los niveles directivos están en capacidad de decidir si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos.

La identificación antes indicada permitirá al directorio u organismo que haga sus veces y a la alta gerencia de la entidad contar con una visión clara de la importancia relativa de los diferentes tipos de exposición al

riesgo operativo y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, que entre otras, pueden ser: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencias y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Artículo 11.- En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente, será necesario que adicionalmente las instituciones controladas conformen bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo; fallas o insuficiencias incluidas las de orden legal; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que las instituciones controladas consideren necesaria y oportuna, para que a futuro se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo. (artículo renumerado y reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Artículo 12.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las instituciones controladas cuenten con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Artículo 13.- El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente. La función de auditoría interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Artículo 14.- Las instituciones controladas deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008).
Los reportes deberán contener al menos lo siguiente:

14.2 Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución; y,

14.3 Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados. Estos informes deben ser dirigidos a los niveles adecuados de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, entre otros.

Sección V.- Responsabilidades en la administración del riesgo operativo

Artículo 17.- Las responsabilidades del directorio u organismo que haga sus veces, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III “Responsabilidad en la administración de

riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Adicionalmente, el directorio u organismo que haga sus veces tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

17.1 Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;

17.2 Aprobar las disposiciones relativas a los procesos establecidos en el numeral 4.1 del artículo 4;

17.3 Aprobar las políticas, procesos y procedimientos para la administración del capital humano conforme con los lineamientos establecidos en el numeral 4.2 del artículo 4;

17.4 Aprobar las políticas y procedimientos de tecnología de información establecidos en el numeral 4.3 del artículo 4; y,

17.5 Aprobar los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV de este capítulo.

Artículo 18.- Las funciones y responsabilidades del comité de administración integral de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008).

Adicionalmente, el comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

18.1 Evaluar y proponer al directorio u organismo que haga sus veces las políticas y el proceso de administración del riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;

18.2 Evaluar las políticas y procedimientos de procesos, personas y tecnología de información y someterlas a aprobación del directorio u organismo que haga sus veces;

18.3 Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;

18.4 Evaluar y someter a aprobación del directorio u organismo que haga sus veces los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV del este capítulo; asegurar la aplicabilidad; y, cumplimiento de los mismos; y,

18.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de contingencia y de continuidad del negocio.

Artículo 19.- Las funciones y responsabilidades de la unidad de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB- 2008-1202 de 23 de octubre del 2008)

Adicionalmente, la unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

19.1 Diseñar las políticas y el proceso de administración del riesgo operativo;

19.2 Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;

19.3 Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de información, especialmente aquellas relacionadas con la seguridad de la información; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008).

19.5 Analizar, monitorear y evaluar los procedimientos de orden legal de la institución; y, en coordinación con las áreas legales, emitir informes que determinen su real exposición al riesgo legal, los cuales deben ser puestos en conocimiento del comité de administración integral de riesgos. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 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

Riesgo Operativo.- Se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.

Según el **Libro I, Normas Generales Para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X, De la Gestión y Administración de Riesgos, capítulo V.**

Riesgo operativo.- Es entendido como la posibilidad de ocurrencia de pérdidas financieras, originadas por fallas o insuficiencias de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos.

Esta definición incluye el riesgo legal, pero excluye los riesgos sistemáticos y de reputación, así también no se toma en cuenta las pérdidas ocasionadas por cambios en el entorno político, económico y social. Las pérdidas asociadas a este tipo de riesgo pueden originarse en fallas de los procesos, en la tecnología, en la actuación de la gente, y también, debido a la ocurrencia de eventos extremos externos. **Enciclopedia libre Wikipedia (2012: Internet).**

Tomando como referencia a **Patricio Reyes Hiedra (2012:24),** riesgo operativo, se refiere a las pérdidas potenciales resultantes de sistemas inadecuados fallas administrativas, controles defectuosos, fraude o error humano.

Sistema de Gestión de Seguridad de la Información.- El SGSI está diseñado para asegurar controles de seguridad adecuados y proporcionados que protejan adecuadamente los activos de información y den confianza a los clientes y otras partes interesadas. **Alberto G. Alexander (2007: 26)**.

Sistema de Gestión de Seguridad de la Información.- La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la Información**. ISO/IEC 27001:2005, Pag.8**

Seguridad de la Información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella. Según **Libro I, Normas Generales Para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X, De la Gestión y Administración de Riesgos, capítulo V.**

Seguridad de la Información.- La preservación de la confidencialidad y la integridad y la disponibilidad de la información, pudiendo abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. **ISO/IEC 27001:2005, Pag.8**

Cultura._ Es un conjuntos de saberes, creencias y pautas de conducta de un grupo social, incluyendo los medios materiales (tecnologías) que usan sus miembros para comunicarse entre sí y resolver sus necesidades de todo tipo. **Enciclopedia libre Wikipedia (2012: Internet)**

Según el artículo publicado por **IT- Insecurity (2009: Internet)**, la cultura de seguridad de la información se basa en que tan bien una organización es capaz de gobernar y administrar los incidentes que se presentan. Cómo se enfrenta la incertidumbre de la falla y a sus efectos inesperados. Una cultura de seguridad de la información que encuentra en la inevitabilidad de la falla la fuente de sus supuestos, es capaz de modificar las prácticas expuestas y en uso, en una realidad concreta que se materializa en comportamientos confiables de las personas.

Es decir, una cultura de seguridad que reconoce en los incidentes o materialización de los riesgos, una forma de actuar y conocer que tan inseguros son, es capaz de construir un lenguaje de seguridad, de percepción, no basado en una visión de invulnerabilidad tecnológica, sino en la confiabilidad de su reacción humana frente a la vulnerabilidad propia de los sistemas. Construir una cultura de seguridad alrededor de los

incidentes, es destruir la falsa sensación de seguridad y diseñar un sistemas preventivo que cree en las buenas prácticas y en el ser humano contingente.

Concepción de la seguridad de la información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor.

Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como:

Crítica: Es indispensable para la operación de la empresa.
Valiosa: Es un activo de la empresa y muy valioso.
Sensible: Debe de ser conocida por las personas autorizadas.

Existen dos palabras muy importantes que son riesgo y seguridad:

Riesgo: Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones.

Seguridad: Es una forma de protección contra los riesgos.

Según información presentada por la **Enciclopedia libre Wikipedia (2012: Internet),** la seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, integridad y confidencialidad de la información.

Diferencias entre seguridad de la Información y Seguridad Informática

Según **Leonardo Camelo (2010: Internet),** el concepto de seguridad de la información no debe ser confundido con el de seguridad informática, son términos usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información; la diferencia entre ellos radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

Seguridad de la Información.- Tiene como propósito proteger la información de una Organización, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

La Seguridad de la Información tiene tres principios fundamentales que son confidencialidad, integridad y disponibilidad de la información.
Su radio de acción cubre Análisis de Riesgos, Seguridad del Personal, Seguridad física y del entorno, Gestión de comunicaciones, Desarrollo y Mantenimiento de Sistemas, Control de Accesos, Gestión de Incidentes, y Continuidad de Negocio entre otros (de acuerdo a la ISO 27000).

Busca mantener el riesgo en la gestión de la información por debajo del nivel asumible por la propia organización.

Seguridad Informática.- Se centra en proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (se centra básicamente en hardware y software), y que estas sean utilizadas de la manera indicada por la Organización.

Su análisis de riesgos se centra en vulnerabilidades del hardware o software, y llevar el nivel de riesgo a nivel aceptable por la organización.

La psicología de la seguridad de la información

Comenta **Shostack y Stewart (2008: Internet),** en su libro que, un verdadero profesional de la seguridad de la información toma mejores decisiones analizando los incidentes de pérdidas de datos, dado que allí encuentra lecciones que la inseguridad le sugiere y no solamente en el reclamo justo de la administración por la pérdida de los mismos.

Esta posición algo extraña, dado que el responsable de la seguridad se expone todo el tiempo por cuenta de la inseguridad, en este sentido, resulta todo un acierto revisar la perspectiva de la seguridad desde la visión psicológica y de percepción de la misma. La seguridad es una sensación, una manera de percibir un cierto nivel de riesgo. Algunas personas son más propensas al riesgo, mientras que otras son más conservadoras. Mientras las primeras gustan del desafío y la vida en los límites, las otras, buscan medir sus pasos y analizar sus posibilidades antes de actuar. Cualquiera que sea el perfil, los dos buscan siempre confrontar la inseguridad para sacar el mejor provecho de ella.

Se deben establecer perfiles de riesgo propios de cada persona, los que permitan establecer mecanismos de control que, no lo limiten en el hacer y le permitan realizar el trabajo con flexibilidad; pero al mismo tiempo, reconocer en el entorno corporativo la “falsa sensación de seguridad” que sugieren los constantes ejercicios de aseguramiento, para mantener una posición proactiva en el tema.

Incorporar en los diseños de seguridad de la información estas conclusiones, permite comprender la inseguridad como una función de la percepción y tendencias humanas por el riesgo, lo cual lleva a visualizar

la configuración de controles y seguridades, que por un lado permitan un libre actuar de las personas en contornos de protección mínimos requeridos y por otro, le permitan al individuo recordar la responsabilidad en el uso de la información dentro y fuera de la organización.

La psicología de la seguridad informática debe estar animada por la constante evolución de la percepción del individuo sobre la protección de los activos, como una manera de incorporar en la gestión de la inseguridad, esa variable que impacta los resultados propios del responsable de la seguridad y su reporte a la alta gerencia: ser más o menos vulnerables.

Crear cultura en seguridad de la información

Involucra inculcar conocimientos que actualmente son indispensables para poder realizar correctamente el trabajo de las personas que manejan herramientas informáticas y trabajan con datos e información.

Debido a que, normalmente, la tarea es relativamente nueva en las organizaciones, entidades o empresas, por lo que se debe poner el empeño para conseguir esta culturización.

Muchas veces se puede llegar a entender que cualquier decisión tomada para cumplir unos mínimos de seguridad de la información puede interpretarse como una traba al trabajo cotidiano de ciertos sectores. Por este motivo, nunca se debe de caer en la tentación de hacer cumplir ciertas directrices sin saber dar una explicación convincente, sin saber escuchar otras opiniones y sin analizar los inconvenientes que se pueden generar, en definitiva sin consensuar la mejor solución para los problemas.

Es por esto, que la persona responsable de la seguridad de la información, debe esforzarse en explicar muy bien los motivos que conducen a marcar unas pautas y unas formas de trabajar.

Política de seguridad de la Información

Según un artículo publicado por **Jordi Solá Sebastiá (2004: Internet),** esta lenta pero progresiva culturización debe llegar a toda la estructura de la entidad. Empieza por la dirección, que es la que tiene que apoyar sin vacilaciones las políticas a seguir.

Política que tiene que estar escrita con claridad y aplicada sin excepciones. A pesar de todo, se entiende que tiene que existir la flexibilidad y capacidad para revisarla cuando sea imprescindible y necesario, para ir adaptándola a los cambios de la propia organización, a la evolución de las tecnologías que el mercado cada día pone a disposición, y a las nuevas vulnerabilidades que pueden surgir en un mundo cambiante y evolutivo.

Una vez que la política de seguridad está aprobada por la dirección, quienes deben cumplirla son todas las personas y estamentos que configuran la organización.

En este momento es cuando hay que saber explicar y hacer comprender el por qué se ha marcado esa política concreta y no otra.

Para conseguir el cumplimiento, uno de los objetivos profesionales es saber transmitir la información y explicaciones pertinentes.
Una persona informada, formada y culturizada, sabrá comprender por qué se dictan ciertas normas y por qué es necesario cumplirlas, y no sólo por

el único motivo de: “porque alguien lo ha dicho”, “porque así está escrito”, o peor todavía, “porque sí”.

Se ha comentado muchas veces, que la formación es muy importante. Así es y así debe ser; pero esta formación debe llevar a adquirir los conocimientos necesarios para tener cultura de la seguridad. No se trata de saber, como ocurría en la escuela para poder aprobar; lo importante es poder transmitir el saber para poder razonar, valorar y, en consecuencia, actuar.

La propia cultura de la seguridad debe llevar a incrementar bidireccionalmente la transmisión de información entre usuarios y administradores de la seguridad, transmisión de información que debe ayudar a encontrar posibles incidencias detectadas en el cotidiano uso de la información y de las tecnologías.

2.4.1.2. Marco conceptual variable dependiente

Administración de la Información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes; **Libro I, Normas Generales Para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X, De la Gestión y Administración de Riesgos, capítulo V.**

Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones. Según **Libro I, Normas Generales Para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X, De la Gestión y Administración de Riesgos, capítulo V.**

Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información prestablecida. Según **Libro I, Normas Generales Para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X, De la Gestión y Administración de Riesgos, capítulo V.**

Confidencialidad.- Es la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados. Según **ISO/IEC (Organización Internacional de Estandarización/ Organización Internacional Electrotécnica) 2001:2005, Pag.8**

Dicho de otro modo, es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

La confidencialidad también se refiere a un principio ético asociado con varias profesiones (por ejemplo, medicina, derecho, religión, psicología profesional, y el periodismo); en este caso, se habla de secreto profesional. En ética, y (en algunos lugares) en Derecho, concretamente en juicios y otras formas de resolución de conflictos legales, tales como la mediación, algunos tipos de comunicación entre una persona y uno de estos profesionales son privilegiados y no pueden ser discutidos o divulgados a terceros. En las jurisdicciones en que la ley prevé la confidencialidad, por lo general hay sanciones por su violación.

La confidencialidad de la información, constituye la piedra angular de la seguridad de la información en corporaciones de hoy en día. La llamada burbuja de confidencialidad restringe los flujos de información, con consecuencias tanto positivas como negativas.

Confidencialidad es la cualidad de que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos. Se trata de una

propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas.

Cuando se produce información confidencial (una carta, un documento, un informe, etc.), los responsables deciden quién o quiénes tienen derecho a acceder a los datos. Los recaudos a tomar para garantizar dicha confidencialidad dependerán del contexto.

Un hombre que quiere mandar una carta a su novia desde el extranjero, se conformará con introducir la nota dentro de un sobre, ya que se supone que nadie más lo abrirá. De todas formas, si alguien lo abriera, no se produciría mayor daño.

Si la información confidencial incluye material que puede poner en riesgo la seguridad de una nación, el nivel de seguridad será mucho mayor. Lo más probable es que el documento en cuestión esté bajo custodia de organismos públicos especializados en lugares secretos, e incluso puede estar escrito en clave.

La confidencial de la información digital (como un correo electrónico) también puede protegerse, aunque no con medidas físicas, sino con mecanismos de cifrado y otras herramientas virtuales.

En algunas profesiones y oficios, la confidencialidad se asocia a un principio ético.

Riesgo.- Se define “como la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular” (Peltier, 2001).

Amenazas.- Es una indicación de un evento desagradable con el potencial de causar daño. **Alberto G. Alexander (2007: 48).**

Vulnerabilidades.- Son debilidades de seguridad asociadas con los activos de información de una organización. **Alberto G. Alexander (2007: 50).**

Puede considerarse "Una debilidad en un sistema, aplicación o infraestructura o diseño de flujo que puede ser explotada para violar la integridad del sistema." (Peltier, 2001).

Salvaguardas.- Son controles existentes.

2.4.2. Gráficos de inclusión interrelacionados

- **Superordinación conceptual**

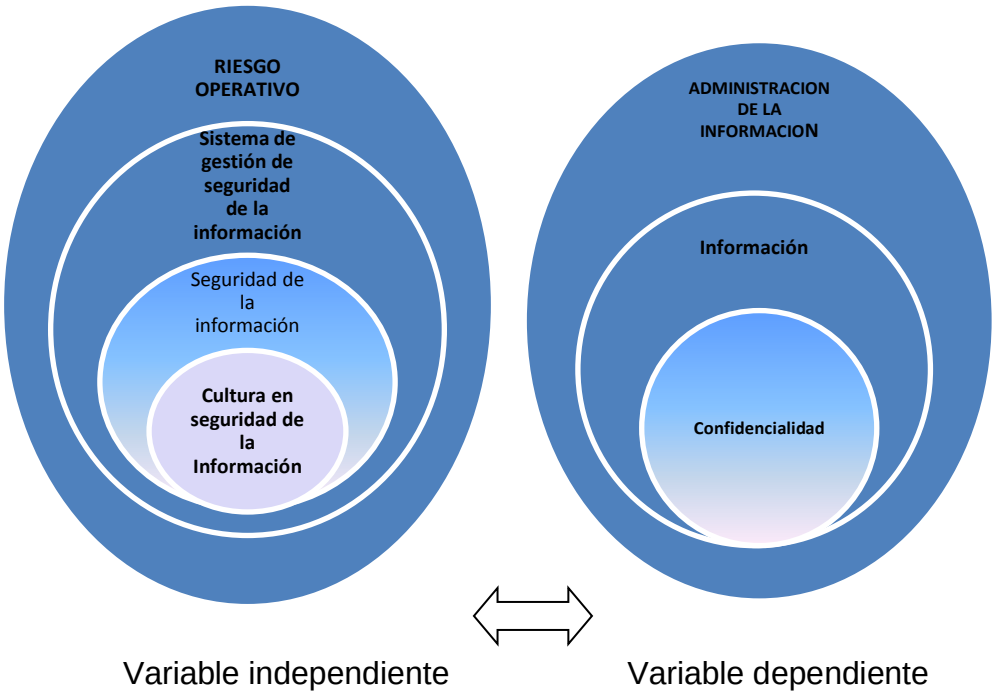


GRAFICO 1. Superordinación Conceptual

Elaborado por: LÓPEZ, Mariela (2012)

- **Subordinación conceptual**

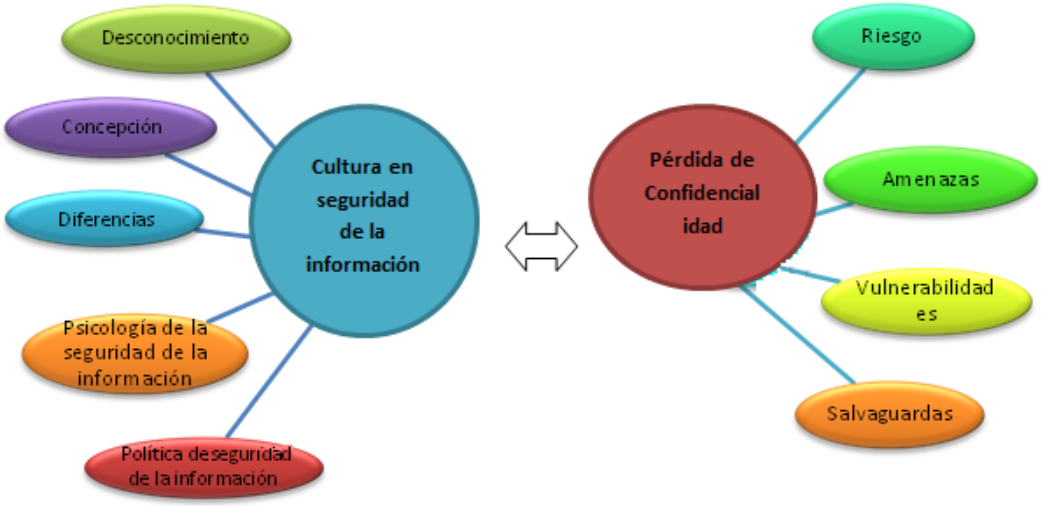


GRAFICO 2. Subordinación conceptual
Elaborado por: LÓPEZ, Mariela (2012)

2.5. Hipótesis

El desconocimiento de la cultura en seguridad de la Información es lo que produce pérdida de confidencialidad en Unifinsa.

2.6. Señalamiento de variables de la hipótesis

- **Variable independiente:** desconocimiento de la cultura en seguridad de la información
- **Variable dependiente:** pérdida de confidencialidad
- **Unidad de observación:** Unifinsa
- **Términos de relación:** es lo que produce, en..

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Enfoque

La presente investigación es predominantemente cuantitativa.

Según información presentada por la **Enciclopedia libre Wikipedia (2009: Internet),** la investigación cuantitativa es un método de investigación basado en los principios metodológicos de positivismo y neopositivismo y que adhiere al desarrollo de estándares de diseño estrictos antes de iniciar la investigación. La investigación cuantitativa desarrolla y emplea modelos matemáticos, teorías e hipótesis que competen a los fenómenos naturales.

En la presente investigación, se buscó las causas y explicación de los hechos que se estudia, y se determinó la relación entre la cultura en seguridad de la información y la confidencialidad.

3.2. Modalidad básica de la investigación

3.2.1. Investigación de campo

Se utilizó la investigación de campo, debido a que esta investigación se realizó en el lugar de los hechos es decir en Unifinsa de la ciudad de

Ambato en el año 2011, donde se recogió información de primera mano del universo involucrado a través de técnicas e instrumentos.

La investigación de campo, permitió reunir datos evidentes de la realidad actual de Unifinsa con la finalidad de diagnosticar el nivel de cultura en seguridad de la información y determinó la relación con la confidencialidad.

3.2.2. Investigación bibliográfica-documental

Se utilizó la investigación bibliográfica documental con el objetivo de profundizar diferentes enfoques, criterios y conceptos, utilizando libros, documentos, revistas, periódicos, con el fin de recopilar toda la información necesaria para la investigación.

La investigación bibliográfica-documental, permitió la recolección de información, datos y fórmulas que se encuentran en los textos y en la Web como aporte científico y como soporte técnico para fundamentar la investigación en Unifinsa.

3.3. Nivel o tipo de investigación

Este proyecto se apoyó sobre bases de una investigación:

3.3.1. Investigación exploratoria

Se utilizó la investigación exploratoria porque permitió sondear el problema, generar hipótesis nuevos métodos, objetivos que son básicos en este tipo de investigación.

En este caso la exploración permitió obtener nuevo datos y elementos que pueden conducir a formular con mayor precisión las preguntas de investigación conducentes al planteamiento de una hipótesis: cuando se desconoce al objeto de estudio resulta difícil formular hipótesis acerca del mismo.

Según **Frank Morales (2010: Internet),** la función de la investigación exploratoria es descubrir las bases y recabar información que permita como resultado del estudio, la formulación de una hipótesis. Las investigaciones exploratorias son útiles por cuanto sirve para familiarizar al investigador con un objeto que hasta el momento le era totalmente desconocido, sirve como base para la posterior realización de una investigación descriptiva, puede crear en otros investigadores el interés por el estudio de un nuevo tema o problema y puede ayudar a precisar un problema o a concluir con la formulación de una hipótesis.

3.3.2. Investigación descriptiva

Tomando como referencia a **Frank Morales (2010: Internet),** la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino busca conocer la realidad del problema de la fuga de información.

Los investigadores recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

3.3.3. Investigación explicativa

Según **Frank Morales (2010: Internet),** la investigación explicativa se encarga de buscar el ¿por qué? de los hechos mediante el establecimiento de relaciones causa-efecto.
En la presente investigación se determinó causas como:

Monitoreo inadecuado de políticas de seguridad de la información, inadecuado número de funcionarios para el monitoreo, deficiente cultura en seguridad de la información, inoportuna capacitación al usuario final, inadecuada identificación del riesgo, controles de seguridad inadecuados

La investigación explicativa intenta dar cuenta de un aspecto de la realidad, explicando su significatividad dentro de una teoría de referencia, a la luz de leyes o generalizaciones que dan cuenta de hechos o fenómenos que se producen en determinadas condiciones.

3.4. Población y muestra

3.4.1. Población

Es el conjunto de todos los individuos (objetos, personas, eventos, etc.) en los que se desea estudiar el fenómeno. Éstos deben reunir las características de lo que es objeto de estudio.

La población analizada durante el año 2011 fue de 76 empleados de la Financiera Unifinsa, adicionalmente información proporcionada por la Coordinadora de Gestión de Talento Humano y Oficial de Seguridad de la Información.
No se presentó la nómina de los colaboradores de la empresa debido a que se encuentra bajo sigilo, reserva y confidencialidad.

3.4.2. Muestra

En esta investigación no se estableció el tamaño de la muestra en virtud de que la población universo es finita e inferior a 100 individuos

3.5. Operacionalización de variables

Siguiendo a **Luis Herrera E. y otros (2002: 166-170**) la operacionalización de hipótesis es un procedimiento por el cual se pasa del plano abstracto de la investigación a un plano concreto, traduciendo cada variable de la hipótesis a manifestaciones directamente observables y medibles, en el contexto en que se ubica el objeto de estudio, de manera que oriente la recolección de información.

Como modelo de operacionalización de variables, se puede sugerir los siguientes pasos:

- Del marco teórico inicial se deriva la conceptualización de la variable, la cual se escribe en la primera columna de la matriz. La conceptualización incluye solo categorías que interesa operacionalizar. Responde a la pregunta: ¿Cuáles son los elementos esenciales de la variable conceptualizada? Las categorías se escriben en la segunda columna. En caso de que las categorías sean muy generales se aumenta otra columna para las subcategorías.

- Para cada categoría se determinan sus indicadores, es decir, elementos directamente observables y medibles que reflejan la presencia y acción de la categoría en un contexto delimitado. Los indicadores que se escogen deben ser significativos para la investigación. Se escriben en la tercera columna.

- Por cada indicador se formulan ítems básicos, que servirán de referentes para diseñar los instrumentos de recolección de información. Estos se escriben en la cuarta columna.

- En una última columna se recomienda fijar las técnicas e instrumentos de recolección.

Responde a la pregunta: ¿Qué instrumentos se aplicarán y a quiénes?
Si la operacionalización es adecuada, de izquierda a derecha de la matriz debe haber una diferenciación progresiva, es decir que el texto de cada columna (a partir de la segunda) sea una subdivisión lógica de la anterior, y así en cada columna disminuye lo abstracto, a la vez que se da un acercamiento progresivo a la realidad observable y medible.

En cierto modo, la operacionalización de las variables se parece a un mapa conceptual, elaborado horizontalmente.

3.5.1. Operacionalización de variable independiente

TABLA 1. Operacionalización de variable independiente

VARIABLE INDEPENDIENTE: Desconocimiento de la cultura en seguridad de la información				
CONCEPTUALIZACIÓN	CATEGORÍAS	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS DE RECOLECCION DE INFORMACION
El desconocimiento de la cultura en seguridad de la información se conceptúa como: Falta de conocimiento, ignorancia de los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.	Confidencialidad de la información	-Personal capacitado -Inducción de seguridad de la información a nuevos colaboradores -Incidentes de seguridad de la información. Análisis de riesgo Evaluación de riesgo Valoración de riesgo Gestión de riesgo Tratamiento de riesgo	¿Usted ha participado en algún programa de capacitación referente a cultura en seguridad de la información en Unifinsa en el año 2011? ¿Ha asistido a charlas en Unifinsa en el año 2011, acerca de pérdida de confidencialidad? ¿Ha asistido a charlas en Unifinsa en el año 2011, respecto a fuga de información? ¿Necesita Usted recibir capacitación en temas relacionados con Fuga de Información?	Encuesta a colaboradores con Cuestionario 1 (Ver Anexo 2) Registros de Gestión de Talento Humano
			¿Autocalifique su grado de cultura en temas de seguridad de la información? – -Teniendo en cuenta que solo el 20% de los colaboradores han recibido la capacitación en temas relacionados con seguridad de la información. ¿Qué falencias presenta Usted en el proceso?	Encuesta a colaboradores con Cuestionario 1 (Ver Anexo 2)
	Integridad de la información	Información completa y exacta	¿Qué riesgo corre al dejar desprotegido su equipo de cómputo cuando se ausenta de su lugar de trabajo?	Encuesta a colaboradores con Cuestionario 1 (Ver Anexo 2)
	Disponibilidad de la información	Recursos disponibles	¿Indique si la implementación de un plan de tratamiento de riesgo contribuirá al control de la fuga de información en Unifinsa?	Encuesta a colaboradores con Cuestionario 1 (Ver Anexo 2)

Fuente: Investigación de Campo

Elaborado por: LÓPEZ, Mariela (2012)

3.5.2. Operacionalización de la variable dependiente

TABLA 2. Operacionalización de variable dependiente

VARIABLE DEPENDIENTE: Pérdida de Confidencialidad				
CONCEPTUALIZACIÓN	**CATEGORÍAS**	**INDICADORES**	**ITEMS BÁSICOS**	**TECNICAS E INSTRUMENTOS DE RECOLECCION DE INFORMACION**
La pérdida de confidencialidad se conceptúa como: El daño de la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados"	Información	Información pública Información privada Cumplimiento de políticas	¿Ha dejado desprotegido el equipo en horas laborables? ¿Necesita Usted recibir capacitación en temas relacionados con pérdidas de confidencialidad? ¿Conoce Usted las políticas de seguridad de la información referentes a la protección de la información confidencial? ¿Ordene cada uno de los medios de pérdida de confidencialidad que a su criterio genera mayor riesgo en la organización. Considerando que 1 es el de mayor riesgo y 6 es el de menor riesgo?	Encuesta a colaboradores con Cuestionario 1 (Ver Anexo 2) Bitácoras de incumplimiento de políticas de seguridad de la información
	Procesos no autorizados	Procesos Críticos Procesos no Críticos Control de acceso a información confidencial	¿Puede Usted identificar que una información es de carácter confidencial? ¿Se ha impartido charlas en Unifinsa acerca de pérdida de confidencialidad? ¿Conoce usted de algún procedimiento para desechar reportes impresos que contienen información confidencial? ¿El desconocimiento de la cultura en seguridad de la información es lo que produce pérdida de confidencialidad en Unifinsa?	Encuesta a colaboradores con Cuestionario 1 (Ver Anexo 2)

Fuente: Investigación de Campo Elaborado por: LÓPEZ, Mariela (2012)

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. Recolección de información

Contempla estrategias metodológicas requeridas por los objetivos e hipótesis de investigación, de acuerdo con el enfoque escogido, considerando los siguientes elementos:

Definición de los sujetos: personas u objetos que van a ser investigados. Los sujetos a ser investigados son los empleados, Coordinadora de Gestión de Talento Humano, y Oficial de Seguridad de la Información de Unifinsa.

Selección de las técnicas a emplear en el proceso de recolección de información. La información fue recolectada a través de encuestas y la observación.

Instrumentos seleccionados o diseñados de acuerdo con la técnica escogida para la investigación. El instrumento seleccionado será el cuestionario

Selección de recursos de apoyo (equipos de trabajo). Para el desarrollo de la presente investigación se contó con la guía y el apoyo de Víctor Hugo Abril PHD e Ing. Ernesto Jara, quienes desinteresadamente aportaron con sus valiosos conocimientos.

Explicitación de procedimientos para la recolección de información, cómo se va a aplicar los instrumentos, condiciones de tiempo y espacio, etc.

Las técnicas e instrumentos para la recolección de datos fueron aplicados a todos los componentes de las unidades de observación. Las técnicas que se utilizaron para dar validez al instrumento de investigación fueron el juicio de expertos tanto en investigación científica, como en el campo de Seguridad de la Información.

De acuerdo con **ARY Y RAZA VICH (1992)** "un cuestionario es válido si los datos obtenidos se ajustan a la realidad sin distorsión de los hechos". (p 214) 3.7.

Se recolectó información, mediante la técnica de la encuesta, basada en el cuestionario como instrumento, para evaluar el grado de cultura en seguridad de la Información, la misma que fue dirigida a los empleados de Unifinsa, de la ciudad de Ambato en el año 2011.

Adicionalmente esta investigación se apoyó en los registros y bitácoras proporcionados por la Coordinadora de Gestión de Talento Humano, y Oficial de Seguridad de la Información de Unifinsa, respectivamente.

TABLA 3. Procedimiento de recolección de información

TÉCNICAS	PROCEDIMIENTO
Encuesta	¿Cómo? A través del Método Inductivo Deductivo
	¿Dónde? La recolección de datos se la realizará en Unifinsa.
	¿Cuándo? La relección de información se la realizará en la cuarta semana de Junio
Observación	Registros y bitácoras proporcionados por la entidad.

Fuente: Investigación de campo
Elaborado por: LÓPEZ, Mariela (2012)

El método inductivo.- es aquel método científico que obtiene conclusiones generales a partir de premisas particulares. Se trata del método científico más usual, en el que pueden distinguirse cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación.

Esto supone que, tras una primera etapa de observación, análisis y clasificación de los hechos, se logra postular una hipótesis que brinda una solución al problema planteado. Una forma de llevar a cabo el método inductivo es proponer, mediante diversas observaciones de los sucesos u objetos en estado natural, una conclusión que resulte general para todos los eventos de la misma clase. **Ramón Ruiz (2007: Internet).**

El método deductivo.- Es un método científico que considera que la conclusión se halla implícita dentro las premisas. Esto quiere decir que las conclusiones son una consecuencia necesaria de las premisas: cuando las premisas resultan verdaderas y el razonamiento deductivo tiene validez, no hay forma de que la conclusión no sea verdadera.
Ramón Ruiz (2007: Internet).

3.7. Procesamiento y análisis

3.7.1. Procesamiento de información

Revisión crítica de la información recogida. Es decir limpieza de información defectuosa: contradictoria, incompleta, no pertinente, etc.

Repetición de la recolección. En ciertos casos individuales, para corregir fallas de contestación.

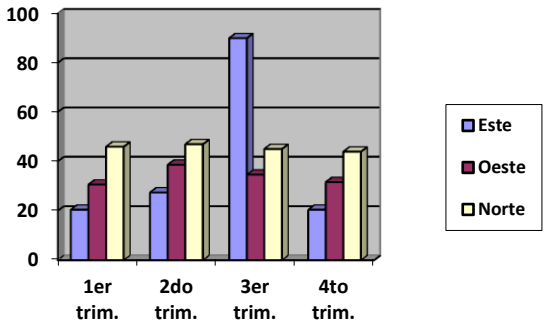
Tabulación o cuadros según variables de cada hipótesis: manejo de información, estudio estadístico de datos para presentación de resultados. Ejemplo de tabla que se utilizó para la cuantificación de los resultados obtenidos con los instrumentos de recolección de información primaria (de campo).

TABLA 4. Cuantificación de resultados

PREGUNTAS	X	y	Z	TOTALES
1				
2				
n				

Fuente: Investigación de campo
Elaborador por: LÓPEZ, Mariela (2012)

Representaciones gráficas. Ejemplo de figura a ser utilizada para la presentación visual porcentual de los resultados cuantificados en la tabla anterior.



Fuente: Investigación de Campo

Elaborador por: LÓPEZ, Mariela (2012)

GRAFICO 3. Representación gráfica de resultados

3.7.2. Análisis e interpretación de resultados

Análisis de los resultados estadísticos. Destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.

Interpretación de los resultados. Con apoyo del marco teórico, en el aspecto pertinente.

Comprobación de hipótesis. El método estadístico de comprobación de hipótesis que se utilizó en el desarrollo de la investigación, fue el Chi cuadrado, para esto se realizó lo siguiente:

-Planteamiento de la hipótesis

-Establecer las reglas de decisión

-Cálculo de X2(Chi cuadrado)

Una variable Chi cuadrado, se define como la suma de n variables normales estandarizadas elevadas al cuadrado.

Características:

-Por definición, una variable 2 adopta valores positivos: 0 " 2 " ".

-La distribución es asimétrica positiva.

-A medida que aumenta el tamaño de la muestra la curva es menos asimétrica, aproximándose a una curva normal.

-Para cada tamaño muestral, se tendrá una distribución 2 diferente.

-El parámetro que caracteriza a una distribución 2 son sus grados de libertad (n-1), originado una distribución para cada grado de libertad,

Establecimiento de conclusiones y recomendaciones.

Explicación del procedimiento de obtención de las conclusiones y recomendaciones. Las conclusiones se derivaron de la ejecución y cumplimiento de los objetivos específicos de la investigación. Las recomendaciones se derivaron de las conclusiones establecidas. A más de las conclusiones y recomendaciones derivadas de los objetivos específicos, se establecieron más conclusiones y recomendaciones propias de la investigación.

TABLA 5. Relación de objetivos específicos, conclusiones y recomendaciones

OBJETIVOS ESPECÍFICOS	CONCLUSIONES	RECOMENDACIONES
Evaluación del grado de cultura en seguridad de la información del personal de Unifinsa de Ambato para la determinación de falencias		
Establecimiento de los tipos de pérdidas de confidencialidad que presenta Unifinsa de la ciudad de Ambato para la determinación del impacto en la organización		
Proponer la implementación de un plan de tratamiento de riesgo de pérdida de confidencialidad de la información en Unifinsa de la ciudad de Ambato		

Fuente: Investigación de Campo
Elaborador por: LÓPEZ, Mariela (2012)

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis e interpretación de los datos

Para la presente investigación, una vez que se recolectó la información se procedió a la revisión y ordenamiento a través de códigos para organizarla de la forma más clara posible, la información fue organizada en categorías, los resultados que se obtuvieron de la tabulación de datos se procedió a presentarlos de una manera gráfica, para mayor comprensión del significado de los datos, se estudió cada uno de los resultados por separado relacionarlos con el marco teórico; dando la pauta para verificar o rechazar la hipótesis del problema de investigación.

4.1.1 Análisis e interpretación de encuesta

LA ENCUESTA FUE REALIZADA A LOS EMPLEADOS DE UNIFINSA DE LA CIUDAD DE AMBATO.

Para la realización de la presente investigación se trabajó con 76 empleados que forman parte de Unifinsa de la ciudad de Ambato. Los resultados de las preguntas se analizan a continuación:

PREGUNTA 1

¿Usted ha participado en algún programa de capacitación referente a cultura en seguridad de la información en Unifinsa en el año 2011?

TABLA 6. Cuadro de Personal Capacitado en Seguridad de la Información en el año 2011.

Respuesta	Frecuencia	Porcentaje
SI	17	22,37%
NO	59	77,63%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

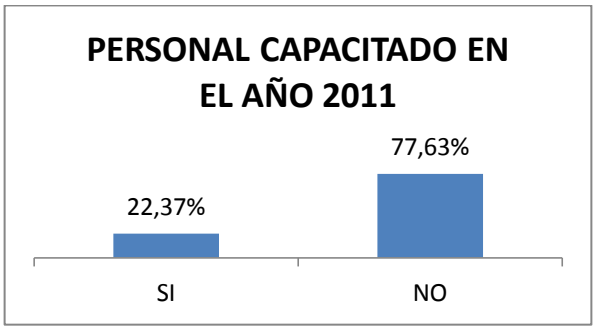


GRAFICO 4. Personal capacitado en el año 2011, en cultura en seguridad de la información

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e interpretación: El 22,37% del personal de Unifinsa, ha participado en un programa de capitación en temas de cultura en seguridad de la información, mientras que el 77,63% no ha participado.

En el año 2011 no se daba la importancia del caso a la cultura de seguridad de la información, añadido a esto la alta rotación de personal y la falta de un control efectivo en los programas de capacitación en temas de seguridad para el nuevo personal, son los causantes de que exista 59 personas de un total de 76 colaboradores que no ha sido capacitado en el tema.

PREGUNTA 2

¿Ha dejado desprotegido el equipo en horas laborables?

TABLA 7. Cuadro de Equipos desprotegidos

Respuesta	Frecuencia	Porcentaje
SI	32	42,11%
NO	44	57,89%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

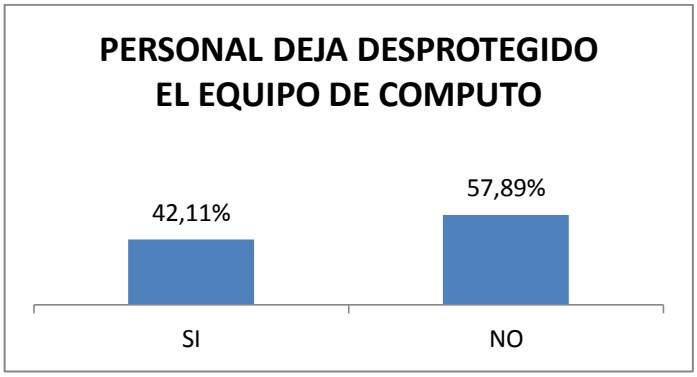


GRAFICO 5. Personal deja desprotegido el equipo de cómputo

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e interpretación: El 42,11% de los empleados deja desprotegido el equipo de cómputo en horas laborables, mientras que el 57,89% lo deja protegido.

De un total de 76 empleados, 44 aún no adquiere el hábito de proteger el equipo cuando abandona su puesto de trabajo, a pesar de que existen políticas de Seguridad de la Información las cuales son difundidas por el Oficial de Seguridad de la Información y conocidas por el personal, los empleados no adquieren conciencia de las responsabilidades que tienen frente al cuidado y la protección de la información.

PREGUNTA 3

¿Qué riesgo corre al dejar desprotegido su equipo de cómputo cuando se ausenta de su lugar de trabajo?

TABLA 8. Cuadro de identificación de riesgo

Respuesta	Frecuencia	Porcentaje
RIESGO ALTO	51	67,11%
RIESGO MEDIO	12	15,79%
RIESGO BAJO	7	9,21%
NINGUN RIESGO	6	7,89%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

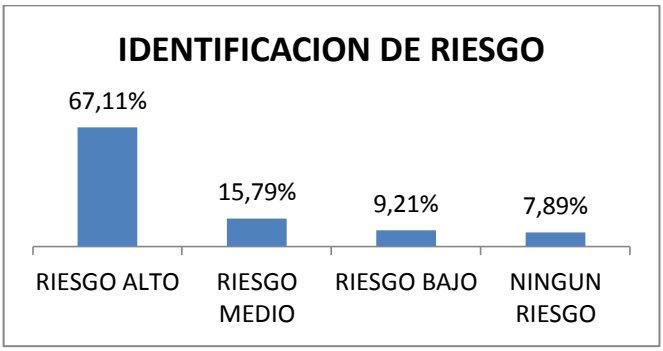


GRAFICO 6. Identificación de Riesgo

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e interpretación: El 67,11%, del personal consideró que el dejar desprotegido el equipo representa un riesgo alto, mientras que el 15,79% indicó que es un riesgo medio, el 9,21% indicó que el riesgo es bajo, y el 7, 89% consideró que no existe ningún riesgo.

De un total de 76 empleados, 51 consideraron que es un riesgo alto, pero a pesar de eso si analizamos la pregunta 2, donde indica que 32 de 76 personas, deja desprotegido el equipo en horas laborables, lo que puede dar lugar a interpretar, es que no existe un compromiso del personal con el cumplimiento de las políticas de seguridad de la información, ni

tampoco se está haciendo conciencia de la responsabilidad que implica el buen tratamiento de la información, esto puede deberse a que el empleado no está capacitado acerca de las consecuencias que acarrea el dejar desprotegido el equipo de cómputo o no existen medidas que sancionen el incumplimiento de esta política. De un total de 76 personas, 12 indicaron que representa un riesgo medio, cabe indicar que estas personas que calificaron como riesgo medio, riesgo bajo y ningún riesgo, no han participado en ninguna capacitación en cultura de seguridad de la información, siendo muy probable que debido al desconocimiento en temas de seguridad de la información hayan calificado como riesgo medio, riesgo bajo y ningún riesgo, el dejar desprotegido su equipo de cómputo cuando un colaborador se ausenta del lugar de trabajo.

PREGUNTA 4

¿Puede Usted identificar que una información es de carácter confidencial?

TABLA 9. Cuadro de identificación de información confidencial

Respuesta	Frecuencia	Porcentaje
SI	63	82,89%
NO	13	17,11%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

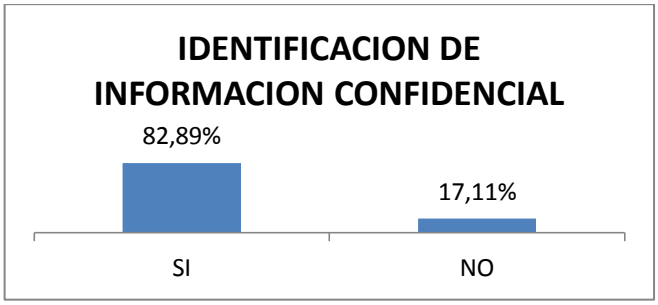


GRAFICO 7. Identificación de Información Confidencial
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 82,89% indicó que puede identificar que una información es de carácter confidencial, mientras que el 17,11% mencionó que no.

De un total de 76 colaboradores, 63 puede identificar que una información es de carácter confidencial, esto puede deberse a la experiencia y a los años de trabajo, más no por una capacitación donde se haya explicado claramente a que información se la debe considerar como confidencial, adicionalmente la ley de sigilo bancario es de gran ayuda. Dentro de los 63 colaboradores, están las áreas de negocio, que por la naturaleza de sus funciones conocen de esta ley, sin embargo 13 personas, no puede identificar si una información es de carácter confidencial, esto también puede deberse ya que no se cuenta con un procedimiento claro para la identificación y el tratamiento de la información confidencial.

PREGUNTA 5

¿Puede Usted identificar que una información es de carácter pública?

TABLA 10. Cuadro de identificación de información pública

Respuesta	Frecuencia	Porcentaje
SI	62	81,58%
NO	14	18,42%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

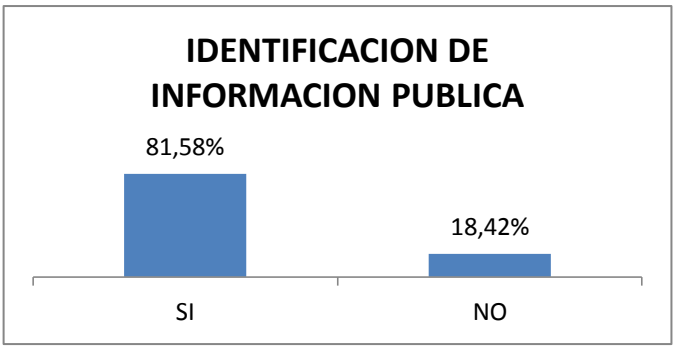


GRAFICO 8. Identificación de Información Pública

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 81,58% del personal, mencionó que puede identificar que una información es de carácter pública, mientras que el 18,42% no.

De un total de 76 colaboradores, 62 personas, mencionaron poder identificar la información pública, hay que tomar en cuenta que es más fácil identificar una información pública ya que puede ser compartida con otras personas sin poner en riesgo a la institución, adicionalmente se puede indicar que la experiencia laboral juega un papel muy importante al momento de identificar la información. 14 de 76 colaboradores mencionaron no poder identificar si una información es de carácter pública, esto puede deberse a que no existe un etiquetado en la información que se maneja dentro de la institución y que todo el personal lo conozca e identifique el tipo de información que maneja, ayudando a evitar errores de manejo de información por desconocimiento.

PREGUNTA 6

¿Ha asistido a charlas en Unifinsa en el año 2011, acerca de pérdida de confidencialidad?

TABLA 11. Cuadro de personal que ha asistido a charlas de pérdida de confidencialidad en el año 2011.

Respuesta	Frecuencia	Porcentaje
SI	15	19,74%
NO	61	80,26%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

GRAFICO 9. Personal que ha asistido a charlas de pérdida de confidencialidad en el año 2011.

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 19,74%, ha asistido a charlas de pérdida de confidencialidad en el año 2011, mientras que el 80,26% no lo ha hecho.

Únicamente 15 de 76 personas, ha asistido a charlas de pérdida de confidencialidad esto puede deberse a que los colaboradores no se interesan en estos temas, o no existe un control adecuado cuando se imparte capacitaciones, lo cual es un problema ya que la capacitación debe ser continua y obligatoria además se debe tomar en cuenta a todo el personal de Unifinsa. De un total de 76 personas, 61 mencionaron no haber participado en ninguna charla referente a este tema, lo que evidencia que no hay un procedimiento controlado de capacitación en temas de seguridad de la información.

PREGUNTA 7

¿Necesita Usted recibir capacitación en temas relacionados con pérdidas de confidencialidad?

TABLA 12. Cuadro de capacitación requerida, referente a pérdida de confidencialidad.

Respuesta	Frecuencia	Porcentaje
SI	64	84,21%
NO	12	15,79%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

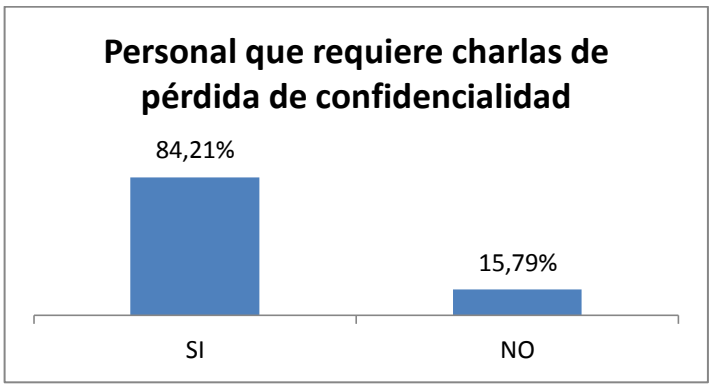


GRAFICO 10. Personal que requiere charlas de pérdida de confidencialidad.
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 84,21%, indicó que necesita participar en charlas referentes a pérdida de confidencialidad, el 15,79% indicó que no.

64 de 76 colaboradores, estuvieron consciente de que requieren participar en charlas de pérdida de la confidencialidad, mientras que 12 de 76 colaboradores indicaron que no requiere, esto se debe al desconocimiento de la importancia de este tema o al desinterés en los asuntos de la empresa.

PREGUNTA 8

¿Ha asistido a charlas en Unifinsa en el año 2011, respecto a fuga de información?

TABLA 13. Cuadro de personal que ha asistido a charlas respecto a fuga de información en el año 2011.

Respuesta	Frecuencia	Porcentaje
SI	10	13,16%
NO	66	86,84%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

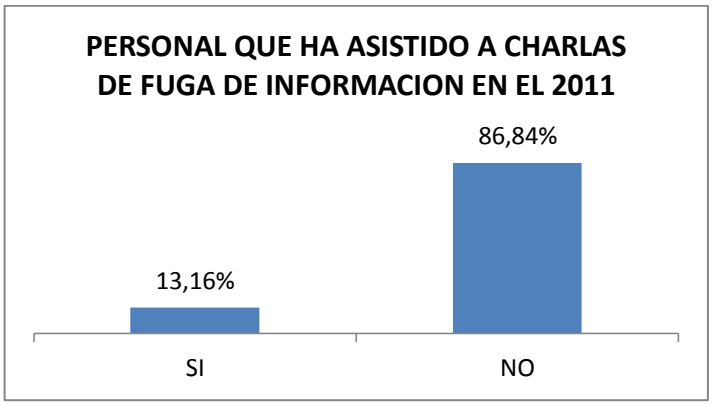


GRAFICO 11. Personal que ha asistido a charlas respecto a fuga de información en el año 2011.

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 13,16%, ha participado en charlas respecto a fuga de información, pero el 86,84% no.

Únicamente 10 de 76 colaboradores, han asistido a charlas de fuga de información, esto genera una gran brecha de desconocimiento, todo el personal debe ser tomado en cuenta en este tipo de capacitaciones, ya que el desconocimiento puede dar lugar a cometer errores involuntarios.

PREGUNTA 9

¿Necesita Usted recibir capacitación en temas relacionados con Fuga de Información?

TABLA 14. Cuadro de capacitación requerida, referente a fuga de información.

Respuesta	Frecuencia	Porcentaje
SI	67	88,16%
NO	9	11,84%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

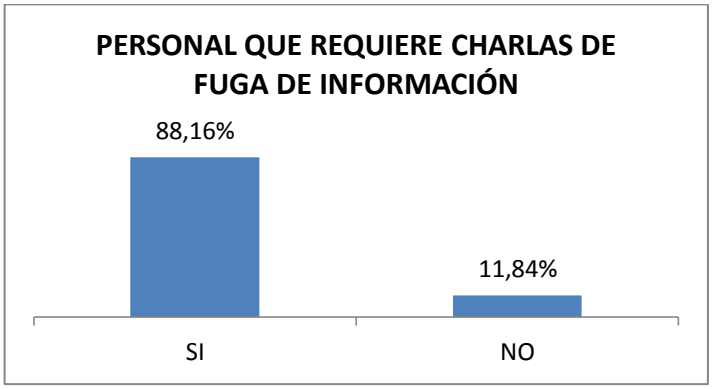


GRAFICO 12. Personal que requiere charlas de fuga de información
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 88,16%, indicó que necesita participar en charlas referentes a fuga de información, el 11,84% indica que no.

De un total de 76 colabores, 67 estuvieron conscientes de que requieren participar en charlas de fuga de información, esto puede interpretarse que el personal tiene predisposición y está consciente que le falta conocimiento en el tema, mientras que 10 de 76 colaboradores indicaron que no requieren, esto puede deberse al desconocimiento del tema y su importancia, es por esto que la capacitación y evaluación continua son una herramienta fundamental para evitar el desconocimiento en el personal.

PREGUNTA 10

¿Conoce Usted las políticas de seguridad de la información referentes a la protección de la información confidencial?

TABLA 15. Cuadro de políticas de protección de información confidencial

Respuesta	Frecuencia	Porcentaje
SI	50	65,79%
NO	26	34,21%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

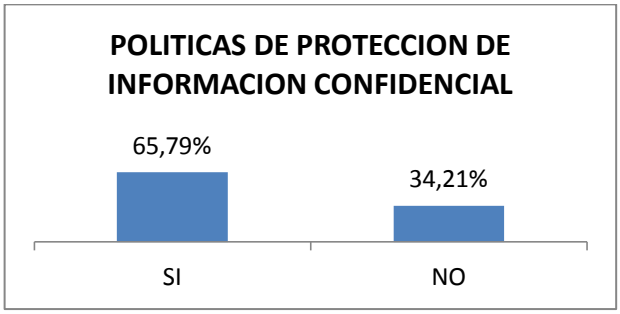


GRAFICO 13. Políticas de protección de información confidencial
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 65,79%, conocía las políticas de seguridad referente a la protección de la información confidencial, pero un 34,21%, del personal las desconocía.

De un total de 76 colaboradores, 50 mencionaron que si conocen de las políticas de la protección de información confidencial, pero 26 de 76 colaboradores la desconocen, esto puede deberse a que existe un problema en el mecanismo de difusión de políticas de seguridad ya que no está llegando la información a todo el personal y como consecuencia se produce el desconocimiento.

PREGUNTA 11

¿Conoce usted de algún procedimiento para desechar reportes impresos que contienen información confidencial?

TABLA 16. Cuadro de personal que conoce procedimiento para desechar reportes impresos que contienen información confidencial

Respuesta	Frecuencia	Porcentaje
SI	27	35,53%
NO	49	64,47%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

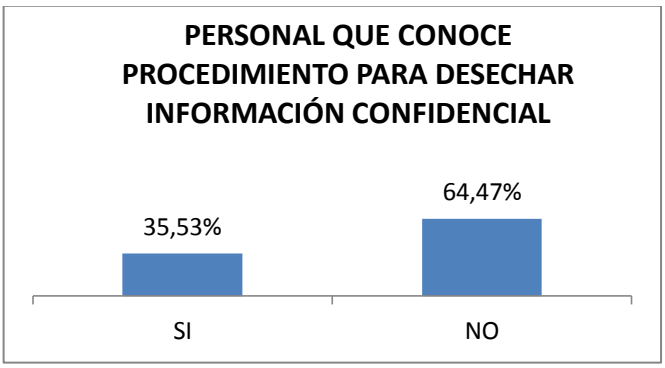


GRAFICO 14. Personal que conoce procedimiento para desechar información confidencial
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 35,53% del personal conocía el procedimiento para desechar reportes impresos que contiene información confidencial, mientras que el 64,47% desconoce del tema.

El hecho de que 49 de 76 colaboradores, haya desconocido del procedimiento, se debe a que no existe un procedimiento formal, que indique al colaborador cómo desechar información confidencial, es muy probable, que 27 personas hayan respondido, que sí conocía de un procedimiento, porque fueron instruidos por su jefe inmediato, más no porque exista realmente un procedimiento para desechar información confidencial.

PREGUNTA 12

¿Autocalifique su grado de cultura en temas de seguridad de la información? Encerrar el número en un círculo.

TABLA 17. Cuadro que indica el grado de cultura del personal de Unifinsa en temas de seguridad de la información.

Respuesta	Frecuencia	Porcentaje
(1-5) BAJO	20	26,32%
(6-10) MEDIO	47	61,84%
(11-15) ALTO	9	11,84%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

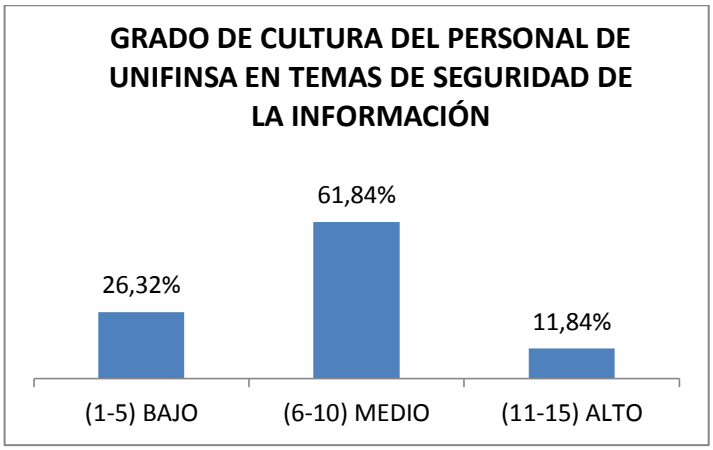


GRAFICO 15. Grado de cultura del personal de Unifinsa en temas de seguridad de la información.

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 26,32% del personal indicó que su nivel en cultura en seguridad de la información es bajo, el 61,84% indicó tener un grado de cultura medio, el 11,84% consideró que tiene un alto grado de cultura en seguridad de la información.

Únicamente 9 de 76 colaboradores, mencionaron tener un alto grado de cultura en seguridad de la información, dentro de este porcentaje se encuentra el personal que mencionó haber recibido la capacitación de seguridad de la información en el 2011 (Pregunta 1). Debido a que no ha existido una adecuada capacitación, 47 colaboradores indicaron tener un grado de cultura medio ya que conocía de las políticas de seguridad de la información para garantizar la confidencialidad de la información, mientras que 20 colaboradores indicaron tener un grado bajo de cultura en seguridad de la información, es muy probable que debido a esto el personal haya solicitado charlas a cerca de pérdidas de confidencialidad (Pregunta 7), fuga de información (Pregunta 9).

PREGUNTA 13

Teniendo en cuenta que solo el 20% de los colaboradores han recibido la capacitación en temas relacionados con seguridad de la información. ¿Qué falencias presenta Usted en el proceso?

TABLA 18. Cuadro de falencias del personal de Unifinsa en Seguridad de la información.

Respuesta	Frecuencia	Porcentaje
A) Desconocimiento de las políticas de seguridad de la información	31	40,79%
B) Desinterés en temas de seguridad de la información	9	11,84%
C) Incumplimiento de políticas de seguridad de la información	6	7,89%
D) Todas las anteriores	9	11,84%
E) A y B	5	6,58%
F) B y C	5	6,58%
G) A y C	7	9,21%
H) Ninguna	4	5,26%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

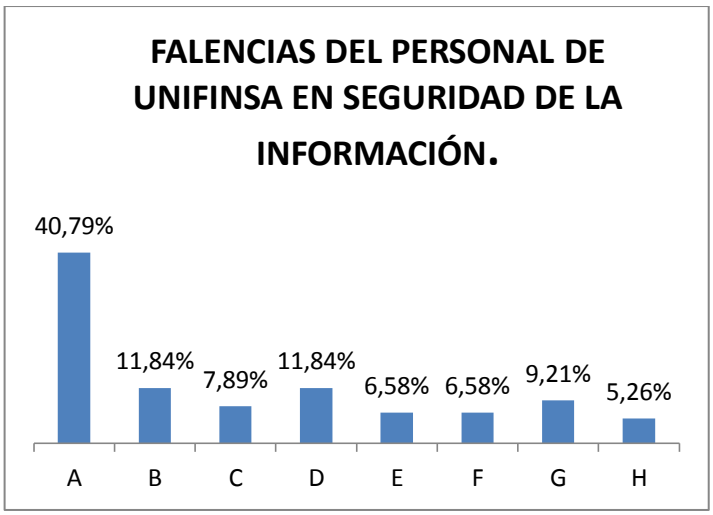


GRAFICO 16. Falencias del personal de Unifinsa en seguridad de la Información

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 40,79% consideró que la falencia que presenta en el proceso de seguridad de la información es por desconocimiento de las políticas de seguridad de la información, el 11,84%, indicó que es desinterés en el tema, el 7,89%, por incumplimiento de las políticas, el 11,84% indicó que es una fusión de desconocimiento, desinterés, e incumplimiento de políticas de seguridad de la información, el 6,58% lo atribuyó al desconocimiento y al desinterés el otro 6,58% indicó desinterés e incumplimiento, mientras que el 9,21%, indica desconocimiento e incumplimiento, finalmente el 5,26% indica no tener falencias en el proceso.

De un total de 76 colaboradores, 31 mencionaron que el desconocimiento de las políticas de seguridad de seguridad es la principal falencia en el proceso, esto se debe a que no existe una correcta comunicación o un medio de difusión por el cual se mantenga informado a toda la institución de las políticas de seguridad, 9 colaboradores consideraron que el desinterés es un gran problema ya que se deben establecer mecanismos para despertar la motivación en los empleados respecto a temas de seguridad, 6 colaboradores indicaron que incumplen las políticas, esto se debe a que se necesita fomentar buenas prácticas junto con una nueva cultura. Adicionalmente, 9 colaboradores indicaron que es una combinación de desconocimiento, desinterés en incumplimiento de políticas de seguridad de la información. 5 colaboradores indicaron que simplemente es desconocimiento y desinterés y otros 5 mencionaron que es desinterés e incumplimiento, 7 colaboradores indicaron que es desconocimiento e incumplimiento mientras que 4 indicaron que no presentan ninguna falencia.

PREGUNTA 14

Ordene cada uno de los medios de información, sujetos a pérdida de confidencialidad que generan mayor riesgo en la organización. Considerando que 1 es riesgo muy alto y 6 es riesgo extremadamente bajo.

TABLA 19. Análisis global de los medios de información, sujetos a pérdida de confidencialidad en orden de importancia.

Medios de Información	Orden de importancia						Total
	1 riesgo muy alto	2 riesgo alto	3 riesgo medio	4 riesgo bajo	5 riesgo muy bajo	6 extremadamente bajo	
documentos fotocpiados	9	14	18	9	14	12	76
documentos impresos	21	10	9	25	9	2	76
discos compartidos	12	6	18	9	19	12	76
salida del personal	6	8	7	11	12	32	76
correo electrónico	18	16	14	13	12	3	76
flash memory discos externos	10	22	10	9	10	15	76

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

Esta pregunta dio origen a 6 tablas y 6 gráficos, como se puede apreciar a continuación:

TABLA 20. Cuadro de medios de pérdida de confidencialidad considerados de riesgo muy alto.

Respuesta	Frecuencia	Porcentaje
documentos impresos	21	27,63%
correo electrónico	18	23,68%
discos compartidos	12	15,79%
flash memory discos externos	10	13,16%
documentos fotocopiados	9	11,84%
salida del personal	6	7,89%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

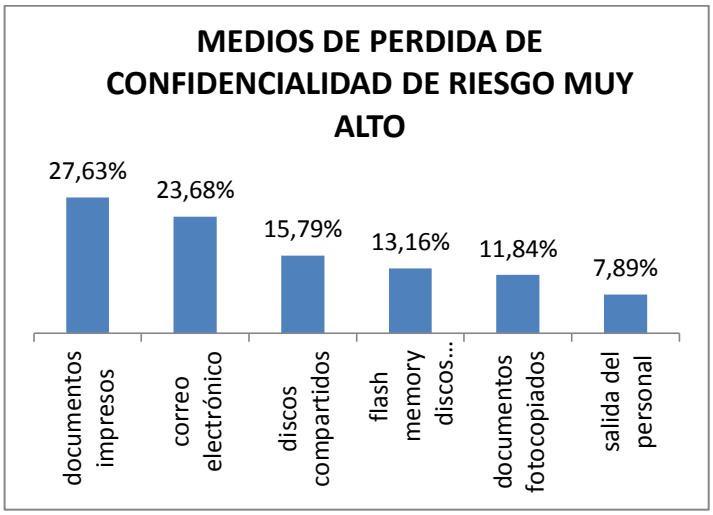


GRAFICO 17. Medios de pérdida de confidencialidad de riesgo muy alto
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 27,63% consideró que el medio de pérdida de confidencialidad, catalogado de riesgo muy alto, son los documentos impresos, el 23,68% indicó al correo electrónico, el 15,79% mencionó los discos compartidos, mientras que el 13,16%, indicó a la flash memory o discos externos, el 11,84% mencionó a los documentos fotocopiados y el 7,89%, a la salida del personal.

De un total de 76 colaboradores, 21 indicaron que el medio de pérdida de confidencialidad catalogado como riesgo muy alto son los documentos impresos, debido a que la institución no cuenta con un sistema de identificación de información confidencial, adicionalmente el personal no cumple con las políticas de mesa limpia dejando abandonados documentos importantes sobre los escritorios en horas no laborables. 18 indicaron al correo electrónico, debido a que es un medio de fácil manejo, siendo un recurso muy utilizado en la empresa, 12 colaboradores indicaron, a los discos compartidos, ya que son un medio donde se coloca información, pero si no existe una concientización por parte de los usuarios y una buena administración por parte de los administradores sobre el buen uso de estos medios de almacenamiento, una persona no autorizada puede tener acceso a la información confidencial, 10 colaboradores indicaron al flash memory o discos externos, debido a que no existe un control del uso de flash memory o discos externos para las laptops o computadores portátiles siendo esta una vulnerabilidad importante. De un total de 76 colaboradores, 9 mencionaron a los documentos fotocopiados, debido a la facilidad que se tiene para sacar fotocopias, cualquier persona a cualquier hora del día o la noche tiene acceso a las fotocopiadoras, 6 colaboradores indicaron a la salida del personal, debido a que es muy difícil controlar la pérdida de confidencialidad cuando el personal se desvincula, a pesar de que existe acuerdos de confidencialidad firmados en el momento de la vinculación.

TABLA 21. Cuadro de medios de pérdida de confidencialidad considerados de riesgo alto.

Respuesta	Frecuencia	Porcentaje
flash memory discos externos	22	28,95%
correo electrónico	16	21,05%
documentos fotocopiados	14	18,42%
documentos impresos	10	13,16%
salida del personal	8	10,53%
discos compartidos	6	7,89%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato

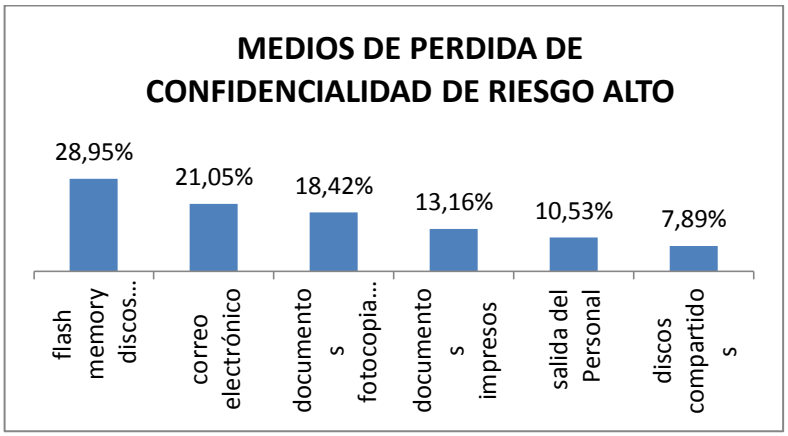


GRAFICO 18. Medios de pérdida de confidencialidad de riesgo alto

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 28,95% consideró que el medio de pérdida de confidencialidad, catalogado de riesgo alto, es la flash memory o discos externos, el 21,05% indicó al correo electrónico, el 18,42%, mencionó a los documentos fotocopiados, mientras que el 13,16% indicó a los documentos impresos, el 10,53% mencionó a la salida de personal y el 7,89% indicó a los discos compartidos.

De un total de 76 colaboradores, 22 indicaron que el medio de pérdida de confidencialidad, de riesgo alto, es la flash memory o discos externos, si bien es cierto la institución cuenta con políticas de bloqueo de los puertos USB, para los computadores de escritorio pero las portátiles no tienen bloqueado dichos puertos, siendo los equipos portátiles los equipos que cuentan con la información más crítica de la compañía.

TABLA 22. Cuadro de medios de pérdida de confidencialidad considerados de riesgo medio.

Respuesta	Frecuencia	Porcentaje
documentos fotocopiados	18	23,68%
discos compartidos	18	23,68%
correo electrónico	14	18,42%
flash memory discos externos	10	13,16%
documentos impresos	9	11,84%
salida del personal	7	9,21%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato

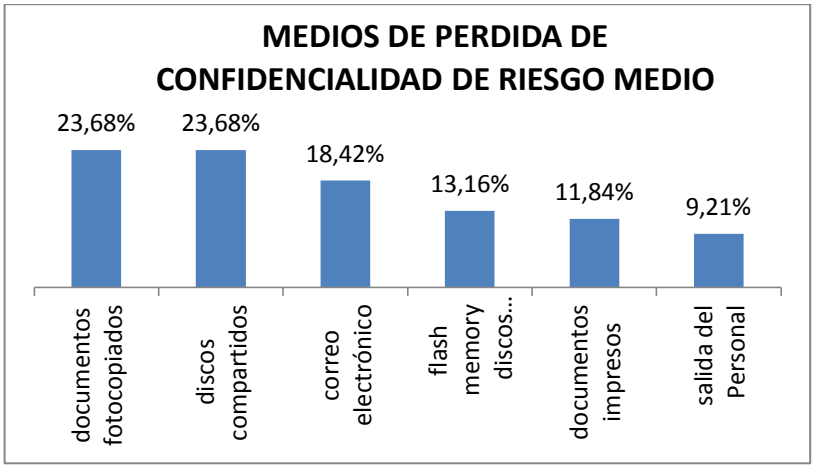


GRAFICO 19. Medios de pérdida de confidencialidad de riesgo medio

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 23,68% consideró que el medio de pérdida de confidencialidad, de riesgo medio son los documentos fotocopiados, el 23,68% indicó a los discos compartidos, el 18,42%, menciona al correo electrónico, mientras que el 13,16% indicó a la flash memory o discos externos, el 11,84% mencionó a los documentos fotocopiados y el 9,21% indicó la salida del personal.

De un total de 76 colaboradores, 18 indicaron que el medio de pérdida de confidencialidad, de riesgo medio son los documentos fotocopiados impresos, debido a que la institución tienen 3 fotocopiadoras, las cuales están disponibles a todo horario sin ningún control de utilización en las horas no laborables y no laborables.

TABLA 23. Cuadro de medios de pérdida de confidencialidad considerados riesgo bajo.

Respuesta	Frecuencia	Porcentaje
documentos impresos	25	32,89%
correo electrónico	13	17,11%
salida del personal	11	14,47%
documentos fotocopiados	9	11,84%
discos compartidos	9	11,84%
flash memory discos externos	9	11,84%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato

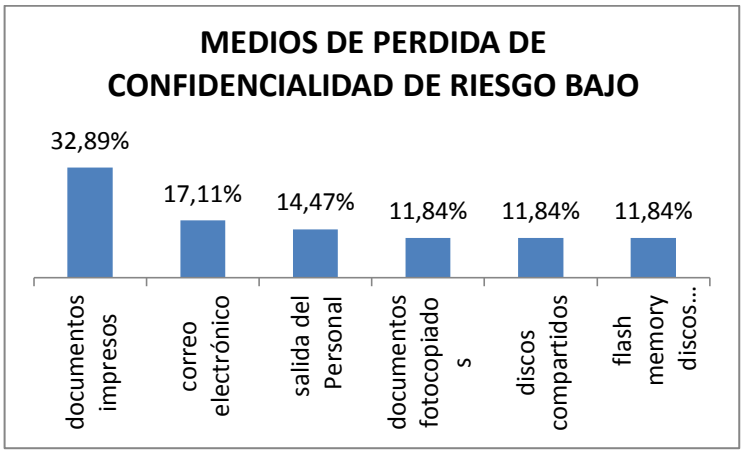


GRAFICO 20. Medios de pérdida de confidencialidad de riesgo bajo

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 32,89% consideró que el medio de pérdida de confidencialidad, catalogado como riesgo bajo son los documentos impresos, el 17,11% indicó al correo electrónico, el 14,47% mencionó la salida del personal, mientras que el 11,84% indicó documentos fotocopiados, el otro 11,84%, indicó los discos compartidos y el 11,84 mencionó a la flash memory o discos externos.

De un total de 76 colaboradores, 25 consideraron que los documentos impresos, son un medio de pérdida de confidencialidad de riesgo bajo, esto se debe a que este grupo de colaboradores no maneja información crítica de la compañía.

TABLA 24. Cuadro de medios de pérdida de confidencialidad considerados riesgo muy bajo.

Respuesta	Frecuencia	Porcentaje
discos compartidos	19	25,00%
documentos fotocopiados	14	18,42%
salida del personal	12	15,79%
correo electrónico	12	15,79%
flash memory discos externos	10	13,16%
documentos impresos	9	11,84%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato

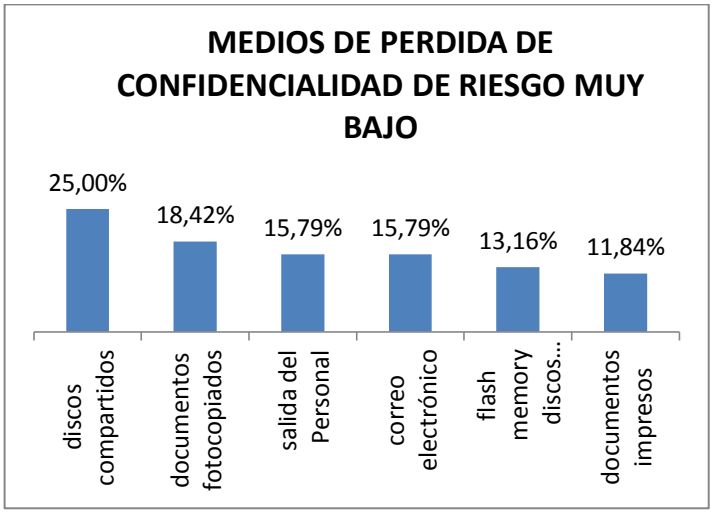


GRAFICO 21. Medios de pérdida de confidencialidad de riesgo muy bajo
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 25% consideró que el medio de pérdida de confidencialidad, catalogado como riesgo muy bajo son los discos compartidos, el 18,42% indicó los documentos fotocopiados, el 15,79% indica la salida del personal, el otro 15,79% mencionó al correo electrónico, el 13,16% indicó a la flash memory y discos externos, el 11,84 indicó los documentos impresos.

De un total de 76 colaboradores, 19 consideraron que los discos compartidos, son un medio de pérdida de confidencialidad de riesgo muy bajo, este riesgo se presenta debido a que no existe una buena práctica en la administración de permisos de las carpetas compartidas.

TABLA 25. Cuadro de medios de pérdida de confidencialidad considerados extremadamente bajo.

Respuesta	Frecuencia	Porcentaje
salida del personal	32	42,11%
flash memory discos externos	15	19,74%
documentos fotocopiados	12	15,79%
discos compartidos	12	15,79%
correo electrónico	3	3,95%
documentos impresos	2	2,63%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato

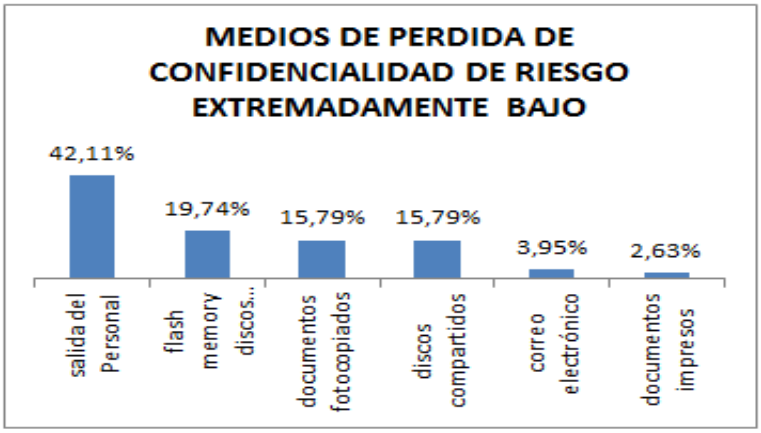


GRAFICO 22. Medios de pérdida de confidencialidad de riesgo extremadamente bajo
Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 42,11% consideró que el medio de pérdida de confidencialidad, catalogado como riesgo extremadamente bajo es la salida de personal, el 19,74% mencionó a la flash memory y discos externos, el 15,79%, indicó a los documentos fotocopiados, el otro 15,79% menciona a los discos compartidos, el 3,95% indicó el correo electrónico, finalmente el 2,63% indicó los documentos impresos.

De un total de 76 colaboradores, 32 consideraron que los documentos compartidos, son un medio de pérdida de confidencialidad de riesgo extremadamente bajo, debido a que anteriormente no existía una alta rotación de personal.

PREGUNTA 15

¿Indique si la implementación de un plan de tratamiento de riesgo contribuirá al control de la fuga de información en Unifinsa?

TABLA 26. Cuadro de implementación del plan de tratamiento de riesgo.

Respuesta	Frecuencia	Porcentaje
SI	73	96,05%
NO	3	3,95%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

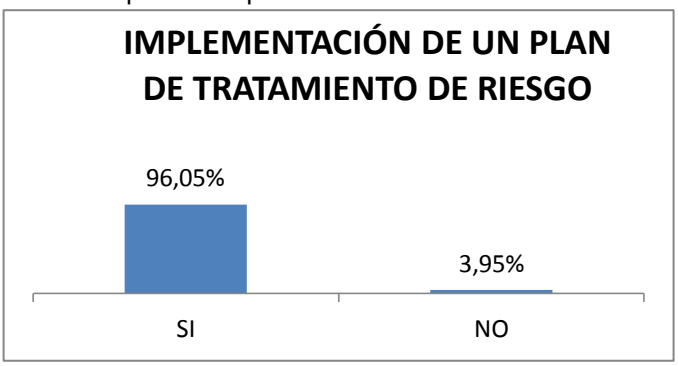


GRAFICO 23. La implementación de un plan de tratamiento de riesgo ayudará al control de la fuga de información

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 96,05%, del personal indicó que la implementación de un plan de tratamiento de riesgo contribuirá al control de la fuga de información, mientras que el 3,95%, de los empleados considera que no.

De un total de 76 colaboradores, 73 indicaron que un plan de tratamiento de riesgo, contribuirá beneficiosamente a la organización, debido a que se evaluaría el riesgo y se establecerían controles mitigantes que ayudarán a reducir el riesgo de fuga de información, el hecho de que 3 de 76 colaboradores no lo haya considerado necesario puede deberse a que los colaboradores desconocen como aportaría un plan de tratamiento de riesgo a la institución. Ya que ellos mencionaron que el sentido común y el compromiso de los empleados bastarían.

PREGUNTA 16

¿El desconocimiento de la cultura en seguridad de la información es lo que produce pérdida de confidencialidad en Unifinsa?

TABLA 27. Cuadro de desconocimiento de la cultura en seguridad de la información.

Respuesta	Frecuencia	Porcentaje
SI	64	84,21%
NO	12	15,79%
TOTAL	76	100,00%

Fuente: Encuesta aplicada al personal de Unifinsa de la ciudad de Ambato.

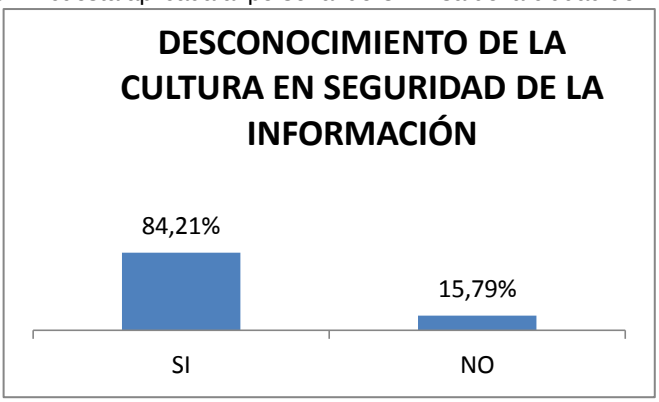


GRAFICO 24. Desconocimiento de la Cultura de la Información

Elaborado por: LÓPEZ, Mariela (2012)

Análisis e Interpretación: El 85,21% del personal indicó que el desconocimiento es la causa principal por las que se produce pérdidas de confidencialidad, mientras que el 15,79% indicó que no.

De un total de 76 colaboradores, 64 estuvieron de acuerdo que el ignorar o desconocer algo respecto a un tema, puede desencadenar en errores involuntarios, un buen plan de capacitación mantendría a los usuarios capacitados y concientizados en temas de cultura en seguridad de la información, logrando que el personal mantenga un correcto tratamiento a la información confidencial, 12 colaboradores indican que no es necesario, esto se debe al desconocimiento de como aportaría un plan de este tipo a la organización.

4.1.2 Análisis e interpretación de registros

Información proporcionada por la Coordinadora de Gestión de Talento Humano.

GRAFICO 25.Registro de número de empleados capacitados en el 2011

Elaborado por: LÓPEZ, Mariela (2012)

El 19,74% ha sido capacitado en temas de seguridad de la información, según el registro de capacitaciones entregado por la Coordinadora de Gestión de Talento Humano, de enero del 2011 a diciembre del 2011

Se registraron únicamente 15 personas de un total de 76 colaboradores los que fueron capacitados en temas de cultura de seguridad de la información, correspondiendo a un 19,74%, y no a 22,37% como se presenta en la encuesta (Pregunta 1). El hecho de que no se capacite a todo el personal puede deberse a que el procedimiento de capacitación no está claramente definido.

Información proporcionada por el Oficial de Seguridad de la Información

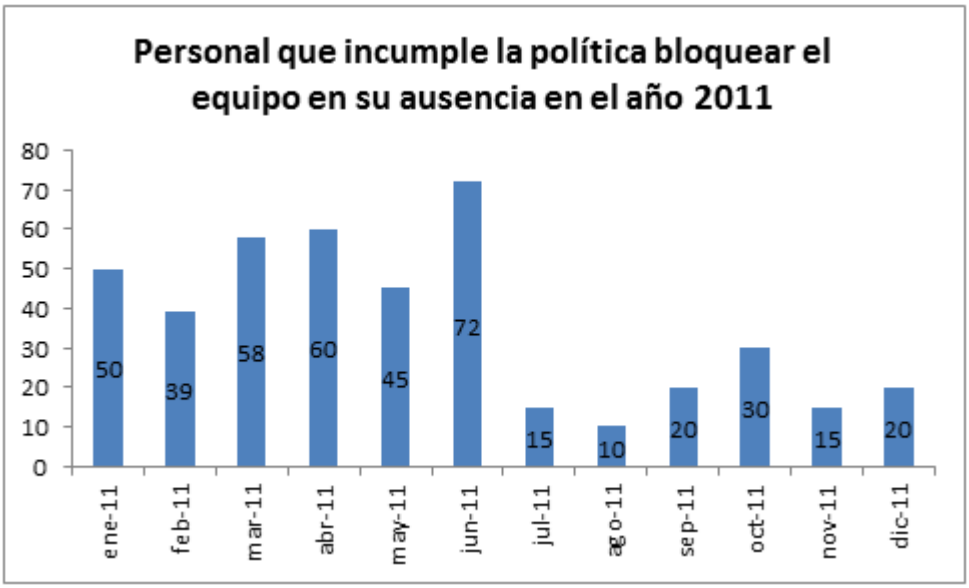


GRAFICO 26. La implementación de un plan de tratamiento de riesgo ayudará al control de la fuga de información

Elaborado por: LÓPEZ, Mariela (2012)

El 38% de los colaboradores, en enero 2011, incumplieron la política que menciona los siguiente “Bloquear el equipo en su ausencia”, en los 6 primeros meses el promedio de incumplimiento fue de un 41,04%, mientras que en el segundo semestre se registró un promedio de 13,93%.

El oficial de seguridad de la información indicó que, las políticas son difundidas al personal vía e-mail, pero no existe un monitoreo que garantice que el empleado haya leído la política de seguridad de la información siendo la capacitación y evaluación continua una herramienta fundamental para evitar el desconocimiento en el personal. A partir del 2 semestre hay una reducción de incumplimientos por parte del personal llegando a un promedio de 18 colaboradores que incumplen esta política, debido a la falta de recursos el Oficial de seguridad de la información indica que esta política no puede ser monitoreada diariamente, pero que el monitoreo lo realiza una vez al mes.

4.2. Verificación de la hipótesis

Se utiliza el Chi-cuadrado como un estadígrafo de distribución libre que permite establecer la correspondencia de valores observados y esperados, permitiendo la comparación global del grupo de frecuencias a partir de la hipótesis que se quiere verificar. Para la combinación se escogieron de la encuesta dos preguntas del tema de investigación considerando las dos variables.

TABLA 28. Frecuencias Observadas

FRECUENCIAS OBSERVADAS			
Alternativas	10. ¿Conoce Usted las políticas de seguridad de la información referentes a la protección de la información confidencial?	1. ¿Usted ha participado en algún programa de capacitación referente a cultura en seguridad de la información en Unifinsa en el año 2011?	TOTAL
SI	50	17	67
NO	26	59	85
TOTAL	76	76	152

Fuente: Encuesta

Elaborado por: LÓPEZ, Mariela (2012)

4.3.1 Formulación de la hipótesis

Hipótesis Nula (H0)

El desconocimiento de la cultura en seguridad de la información no es lo que produce pérdida de confidencialidad en Unifinsa.

Hipótesis alternativa (H1)

El desconocimiento de la cultura en seguridad de la información es lo que produce pérdida de confidencialidad en Unifinsa.

4.3.2 Elección de la prueba estadística

Para la verificación de la hipótesis se escogió la prueba Chi Cuadrado, cuya fórmula es la siguiente:

$$X^2c = \sum_{j=1}^{K} \frac{(O_j - E_j)^2}{E_j}$$

Simbología:

X^2_C= Chi-cuadrado

Σ = Sumatoria

O = Datos observados

E = Datos esperados

4.3.3 Definición del nivel de significación y regla de decisión

El nivel de significación escogido para la investigación fue el 5% (0,05)

Grados de Libertad

Para determinar los grados de libertad se utiliza la siguiente fórmula:

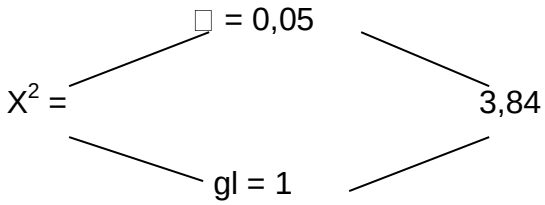
GL = (c-1) (f-1)

GL= (2-1) (2-1)

GL = 1

Grado de significación

□ = 0,05



Al nivel de significación de 0,05 y un (1) grado de libertad (gl) el valor Chi-cuadrado a tabular es 3,84 ($X^2t = 3,84$)

- Regla de decisión:

Se acepta la hipótesis nula si el valor del Chi-cuadrado a calcularse es igual o menor a $X^2t = 3,84$; caso contrario se rechaza y se acepta la hipótesis alternativa.

4.3.4 Cálculo de Chi-cuadrado X^2c

Datos obtenidos de la investigación

TABLA 29. Frecuencias Esperadas

FRECUENCIAS ESPERADAS			
Alternativas	10. ¿Conoce Usted las políticas de seguridad de la información referentes a la protección de la información confidencial?	1. ¿Usted ha participado en algún programa de capacitación referente a cultura en seguridad de la información en Unifinsa en el año 2011?	TOTAL
SI	33,5	33,5	67
NO	42,5	42,5	85
	76	76	152

Fuente: Encuesta

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 30. Cálculo del Chi-cuadrado

Frecuencias Observadas **O**	Frecuencias Esperadas **E**	Desviación **(O - E)**	Deviación cuadrada **$(O - E)^2$**	Desviación cuadrada Estandarizada **$(O - E)^2/E$**
50	33,5	16,5	272,25	8,127
26	42,5	-16,5	272,25	6,406
17	33,5	-16,5	272,25	8,127
59	42,5	16,5	272,25	6,406
			X^2c =	29,065

Fuente: Encuesta

Elaborado por: LÓPEZ, Mariela (2012)

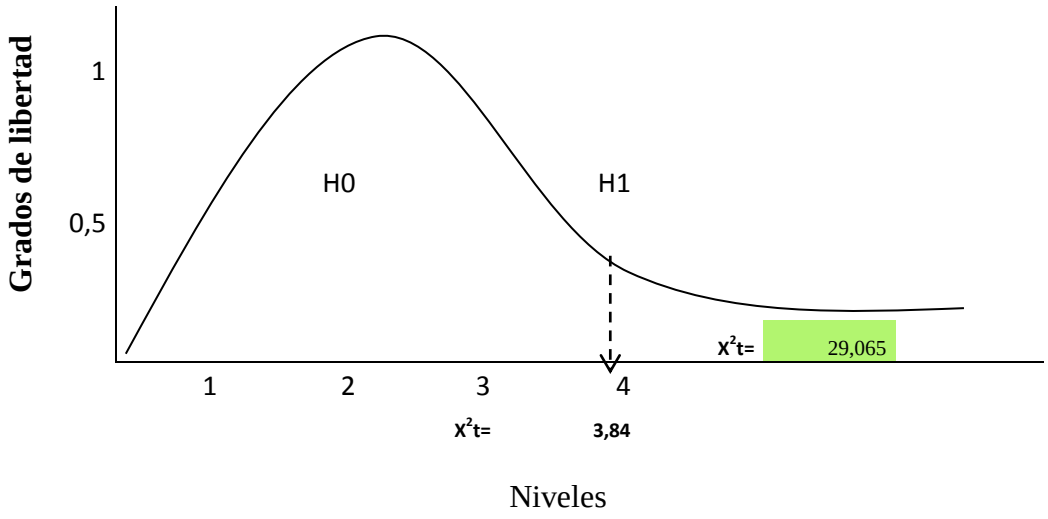


GRAFICO 28. Verificación de la Hipótesis

Elaborado por: LÓPEZ, Mariela (2012)

Conclusión.- El valor de X^2c = 29,065 > X^2t = 3,84 de acuerdo a lo establecido se rechaza la hipótesis nula y se acepta la hipótesis alternativa, es decir que el desconocimiento de la cultura en seguridad de la información es lo que produce pérdida de confidencialidad en Unifinsa.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Después de haber realizado el estudio de la relación de la cultura en seguridad de la información con la pérdida de confidencialidad en Unifinsa de la ciudad de Ambato, se concluye lo siguiente:

Mediante el proceso de investigación, se determinó que el desconocimiento de la cultura en seguridad de la información, es lo que produce pérdida de confidencialidad en Unifinsa, cumpliendo así con la hipótesis planteada, gracias a la colaboración del personal de Unifinsa, a la ayuda de las encuestas y a los registros y bitácoras proporcionados por la coordinadora de gestión de talento humano, y oficial de seguridad de la información, se pudo comprobar la hipótesis.

El 84,21% de los colaborados de Unifinsa, consideraron que el desconocimiento de la cultura en seguridad de la información es lo que produce la pérdida de confidencialidad.

La fuga de la información es una amenaza latente que aqueja a la empresa, debido a una variedad de factores los mismos que deben ser controlados; es por esto, que la cultura en seguridad de la información, cumple un papel muy importante en las organizaciones, en Unifinsa el 61,84% del personal, respondió tener un nivel medio en cultura en seguridad de la información, lo cual, es realmente preocupante, ya que

esto es atribuido a la falta de capacitación y al desconocimiento de políticas de seguridad de la información por parte del personal.
Generalmente, se toman precauciones técnicas para prevenir estas amenazas, olvidando la capacitación de los empleados, siendo este un grave error.

Uno de los medios de pérdida de confidencialidad que fue considerado el más riesgoso en Unifinsa, son los documentos impresos, debido a que no existe un control de impresión de documentos, especialmente de los reportes que son generados del sistema transaccional; adicionalmente, el 4% del personal de Unifinsa, que corresponde al Departamento de Mensajería, y este no cuentan con una capacitación adecuada, porque son excluidos dentro del plan de capacitación de seguridad de la Información; tomando en cuenta que el personal de mensajería, es quién está más en contacto con la información (documentos impresos, documentos fotocopiados etc.), si bien es cierto no utilizan equipos de cómputo, pero tienen constante acceso a todo tipo de documentos de la organización, convirtiéndose esta situación en vulnerable.

Adicionalmente, el correo electrónico es el segundo dentro del grupo de los más riesgos, ya que el personal considera que es el más fácil de usar y no existe ningún mecanismo de detección.

Discos Compartidos, es el tercero dentro del grupo de los más riesgosos, debido a que personal no cumple con las políticas establecidas.

Flash memory o Discos Externos, es el cuarto dentro del grupo de los más riesgosos, el personal consideró que es el medio más fácil de extraer información.

Documentos fotocopiados, es el quinto dentro del grupo de los más riesgos, ya que existen fotocopiadoras las mismas que no son controladas

y cualquier persona puede hacer uso de ellas a cualquier hora del día o noche.

Salida del personal, es el sexto dentro del grupo de los más riesgos a pesar de que existen acuerdos de confidencialidad firmados por los empleados, el riesgo cuando el personal se desvincula de la institución es más difícil de controlar.

Durante el levantamiento de la información se observó que se tiene una idea equivocada de que la seguridad de la información es responsabilidad del departamento de TI (Tecnología de Información), anteriormente conocido como Departamento de Sistemas, la seguridad de la información es responsabilidad de todos, ya que de nada sirve instalar los controles más sofisticados si el usuario no cumple con las medidas básicas de seguridad establecidas, muchas veces se olvida enfocarse en el eslabón más débil de la cadena de seguridad: el factor humano.

Una de las principales obligaciones para la organización es garantizar que su personal actúe de manera correcta, pero el personal capacitado en cultura en seguridad de la información es realmente bajo el 22,37%, situación que es verdaderamente preocupante, debido a las crecientes amenazas en contra de la seguridad de la información

Los empleados descontentos, la venta de información, la venganza, o la creación de nuevas empresas son algunos de los motivos que generan fugas de información, sin dejar de lado la falta de conocimiento, formación o sencillamente errores involuntarios.

El no contar con un método de etiquetado de información, es también un factor importante para determinar un correcto tratamiento de la información, si el empleado o colaborador desconoce qué tipo de información es la que maneja es imposible que pueda dar un buen

tratamiento a la información e identificar si está procediendo de manera incorrecta.

5.2. Recomendaciones

Se recomendó al Oficial de seguridad de la información, la implementación de un plan de tratamiento de riesgo que contribuya al control de la fuga de información en Unifinsa.

Es recomendable considerar a la seguridad de la información como un proceso continuo donde se debe comprometer a todo el personal de la institución, empezando por aspectos tan simples como mantener las contraseñas en secreto, para esto se requiere de una compresión individual y completa donde la misión es educar bajo una cultura consciente y responsable a cerca de los diferentes riesgos y responsabilidades que tiene el empleado frente al tratamiento y protección de la información.

Capacitar al personal en temas de seguridad de la información ayudaría de manera sustancial ya que se evitaría errores involuntarios producidos por desconocimiento.

Establecer políticas de seguridad de la información es una gran ayuda para controlar la fuga de la información ya que el personal conocería cuales son los límites y hasta esta donde puede llegar.

Las consecuencias de la fuga de información pueden ser irremediables y muy negativas pudiendo afectar a la organización, es recomendable centrarse en la prevención de la fuga de información pero también es importante no perder de vista la gestión de incidente, es decir con el fin de

que se minimice adecuadamente el impacto y evitar un empeoramiento de la situación.

Se debe establecer medidas de control para garantizar que no se produzca fuga de información en la organización, en la actualidad la industria de seguridad ofrece un buen número de soluciones de seguridad en forma de productos y servicios, entre los que destacan aquellos destinados específicamente a evitar la fuga de información (DLP) (*Data Lost Prevention* por sus siglas en inglés). La prevención de la fuga de información es un negocio en auge.

CAPÍTULO VI

PROPUESTA

6.1. Datos Informativos

6.1.1. Título

“Implementación de un plan de tratamiento de riesgo de pérdida de confidencialidad de la información en Unifinsa de la Ciudad de Ambato.”

6.1.2. Institución

Unifinsa, una de las sociedades financieras más prestigiosa de la ciudad de Ambato.

Abrió sus puertas el 5 de Agosto del 1994, durante 17 años, ha brindado a sus clientes un servicio de calidad y profesionalismo lo cual la ha convertido en una de las primeras Instituciones Financieras del centro del país y una de las mejores a nivel nacional.

6.1.3. Beneficiarios

Se beneficiarán del tema en investigación lógicamente Unifinsa, y sus empleados adicionalmente cualquier Institución del Sistema Financiero u organización.

6.1.4 Ubicación

Provincia de Tungurahua, Cantón Ambato
Av. Cevallos 15-66 y Mera

6.1.5. Tiempo estimado para la ejecución

La construcción del proyecto tendrá una duración de 8 meses aproximadamente, desde la fecha de su aprobación.

6.1.6. Equipo técnico responsable

Unidad de Riesgos
Oficial de Seguridad de la Información

6.1.7. Costo

$64.000

6.2. Antecedentes de la propuesta

En la actualidad el activo más importante que poseen las empresas es la información, la falta de control sobre la información es un riesgo latente.

Es evidente que un competidor puede estar interesado en conocer nuestros secretos. Pero no es el único que puede estarlo. Un trabajador resentido, un miembro de nuestro propio equipo de trabajo, etc., pueden

estar interesados en determinada información, sea para fines lícitos o ilícitos.

Es muy difícil poder 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.

Como cualquier otro incidente de seguridad, la fuga de información tiene un origen y unas causas principales.

Por otro lado, si el incidente finalmente tiene éxito, tendrá consecuencias que afectarán por un lado a la propia organización, pero también podrán tener impacto sobre grupos externos de usuarios.

El impacto y las consecuencias posteriores a un incidente de fuga de información, es uno de los aspectos que mayor preocupación despierta en las organizaciones, puesto que la filtración de información puede dañar la imagen pública de una empresa generando un impacto negativo para el negocio, además creando un ambiente de desconfianza e inseguridad en el público en general y generar otras consecuencias a terceros, como en el caso de que la información filtrada haga referencia a usuarios o clientes.

Según **Eric Donders O. (2010: Internet),** comenta “que la gestión de riesgos de la información es la aplicación sistemática de políticas, prácticas y procedimientos de Gestión a las tareas de identificar, analizar evaluar tratar y monitorear el riesgo.

Según **INTECO (**Instituto Nacional de Tecnologías de la Comunicación**) (2012: Internet),** comenta que “Las consecuencias de un incidente de fuga de información preocupan enormemente a las empresas y las organizaciones. Un incidente que se hace público, puede causar un

importante daño de imagen o mermar la confianza de los clientes de la entidad, lo que puede llegar a afectar a su negocio."

Comprender las posibles consecuencias es un aspecto esencial y necesario para la gestión de incidentes de fuga de información. A través del estudio de las posibles consecuencias, es posible diseñar una estrategia, de forma que en caso que finalmente se produzca un incidente de fuga de información, sea posible tomar las decisiones adecuadamente, minimizando el impacto, ya sea sobre la propia organización o incluso sobre terceros, ya sean clientes, usuarios o sobre otras organizaciones.

Según **Alberto G. Alexander (2007: 56),** menciona en su libro que, para todos aquellos riesgos donde la opción de reducirlos se ha tomado se deben implementar controles apropiados para poder reducirlos a nivel que se haya definido como aceptable. Es importante mencionar que al haber identificado el nivel de control, conviene considerar los requerimientos de seguridad relacionados con los riesgos.

Y que las estrategias posibles para el tratamiento del riesgo son:

- ✓ Reducción del riesgo
- ✓ Objetivamente aceptar el riesgo
- ✓ Transferencia del riesgo
- ✓ Evitar el riesgo

Un plan de tratamiento de riesgo es esencial dentro de una organización ya que ahí se deciden cuáles son las acciones que se van a tomar en cuenta con los activos de información que están sujetos a riesgos, hay que estar consciente que el riesgo no puede eliminarse, al riesgo se lo puede controlar, asumir, evitar o transferir, la organización es quien escoge la manera más efectiva de protección en función de los requerimientos del negocio y las circunstancias en las cuales la organización necesita operar.

6.3. Justificación

La información es producida y consumida por personas, por ende el factor humano es el principal elemento que la pone en riesgo, por lo que es importante tener un amplio conocimiento de los riesgos que puede correr dicha información y así poder definir lineamiento que pueden resguardarla.

Contar con un plan de tratamiento de riesgo ha permitido mitigar los riesgos identificados relacionados a la fuga de información, ayudando a fortalecer la cultura de administración de riesgo y por ende la cultura en seguridad de la información en función del desarrollo de valores éticos y morales, fomentando en los colaborares la responsabilidad del manejo de información desde la perspectiva de confidencialidad.

Una gestión deficiente, la ausencia de controles, políticas, monitores, son las causas que propician y facilitan un incidente de fuga de información, pero con un plan de tratamiento de riesgos debidamente gestionado, controlado y monitoreado, se mitigarán los riesgos que están sujetos al activo de información.

La clasificación de la información en base a su nivel de confidencialidad, es un aspecto fundamental, ya que si se desconoce el valor que tiene para la organización, el impacto que puede generar su difusión, su nivel de sensibilidad o si es personal o no, sería muy difícil establecer el perímetro dentro del cual puede ser difundida dicha información.

El poder identificar con objetividad que requiere ser protegido ¿por qué?, ¿de qué debe ser protegido? y ¿cómo protegerlo?, ayuda a reaccionar con mayor rapidez ante un incidente de seguridad, estableciendo las causas raíz que lo generaron e implantar las acciones correctivas pertinentes.

La ISO 27001 (*International Standard Organization* por sus siglas en inglés), recomienda a las organizaciones implementar un plan de tratamiento de riesgo, donde se identifique las acciones de la Dirección, los recursos, las responsabilidades y las prioridades adecuadas para gestionar los riesgos de la seguridad de la información.

6.4. Objetivos

6.4.1. Objetivo General

Implementar un plan de tratamiento de riesgo de pérdida de confidencialidad que controle la fuga de información en Unifinsa de la ciudad de Ambato.

6.4.2. Objetivos específicos

Identificar los activos de información que tienen impacto en el negocio por pérdida de confidencialidad.

Realizar un análisis y evaluación del riesgo

Identificar y evaluar las opciones para el tratamiento del riesgo

Seleccionar objetivos de control y controles para el tratamiento del riesgo.

6.5. Análisis de factibilidad

6.5.1. Organizacional

La institución financiera, cuenta con un Oficial de Seguridad de la Información, quien es responsable de preservar la confidencialidad integridad y disponibilidad de la información, este estudio está enfocado únicamente a la confidencialidad de la información.

Tomando en cuenta que la información es un activo, que como otros activos importantes del negocio, tiene valor para la organización, es necesario tener una protección adecuada, como resultado de la creciente interconectividad la información está expuesta a un sin número de amenazas.

6.5.2. Legal

La ley de sigilo, reserva y confidencialidad bancaria en el Art. 88 de la Ley de Instituciones del Sistema Financiero indica.

"Los depósitos y demás captaciones de cualquier índole que se realicen en las instituciones del sistema financiero, estarán sujetos a sigilo bancario, por lo cual las instituciones financieras receptoras de los depósitos y captaciones, sus administradores, funcionarios y empleados no podrán proporcionar información relativa a dichas operaciones sino a su titular o a quien lo represente legalmente.

Las instituciones del sistema financiero podrán dar a conocer las operaciones anteriores, en términos globales, no personalizados ni parcializados, solo para fines estadísticos o de información.

La ley de sigilo es muy clara en el aspecto referente a la confidencialidad de las operaciones activas y pasivas de los clientes, por este motivo es factible este proyecto para que el personal y la Administración conozcan cuáles son sus responsabilidades frente al tratamiento de la información.

6.5.3. Tecnológica

La masificación del uso de la tecnología que posibilita el tratamiento de la información para que pueda ser transmitida, procesada, copiada, almacenada con una rapidez y eficacia increíble, ha representado realmente un gran reto desde el punto de vista de mantener la confidencialidad de la información.

Si bien es cierto controlar la fuga de información no es tarea fácil, en la actualidad la industria tecnológica, ofrece un buen número de soluciones de seguridad en forma de productos o servicios, los mismos que están destinados a la prevención de la fuga de información.

Por otro lado, luego de haber realizado el estudio de investigación referente a la implementación de un plan de tratamiento de riesgo que controle la fuga de información, podemos ratificar que la propuesta es factible.

Adicionalmente, es factible porque se cuenta con los recursos y apoyo necesario para culminar exitosamente la propuesta. Los recursos económicos, el material bibliográfico han jugado un papel muy importante para el buen desarrollo del proyecto.

Los beneficiarios de este estudio serán lógicamente Unifinsa, sus colaboradores y la sociedad.

6.6. Fundamentación

6.6.1 Fundamentación Teórica

Identificación de los activos de información

Los activos de información en la empresa, dentro del alcance del sistema de gestión de seguridad de la información son fundamentales para una correcta implementación del mismo.

El análisis y la evaluación de riesgo en la empresa giran alrededor de los activos de información identificados.

Activo de Información

Un activo de información, para **Alberto G. Alexander (2007: 44-45),** es algo que tiene valor o utilidad para la organización sus operaciones comerciales y su continuidad, por esta razón los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

Según la ISO 17799:2005 (*International Standard Organization* por sus siglas en inglés), Código de prácticas para la gestión de seguridad de la información, un activo de información es “algo a lo que una organización

directamente le asigna un valor y por lo tanto la organización debe proteger".
Además, clasifica a los activos de información en las categorías siguientes:

-Activos de información (datos, manuales de usuario, etc.)
-Documentos de papel (contratos)
-Activos de Software (Aplicación, software de sistemas, etc.)
-Activos Físicos (computadoras, medios magnéticos, etc.)
-Personal (Cliente, personal)
-Imagen de la compañía y reputación
-Servicios (comunicaciones, etc.)

Es fundamental estar conceptualmente claros de qué es un activo de información y conocer sus distintas posibles modalidades, para así realizar un correcto análisis y una evaluación de riesgos.

En la organización, el proceso de identificación y de tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en el proceso y subprocesos que abarca el alcance del modelo.

Propietario del Activo de Información

Un dueño o propietario del activo se entiende aquella persona que tienen una responsabilidad por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos, aprobada por la gerencia.

En otras palabras tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de confidencialidad o destrucción deliberada y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida.
La responsabilidad del propietario debiera ser también la de revisar periódicamente los derechos de acceso y la seguridad. Además de esto, debiera ser útil definir, documentar e implementar reglas para el uso aceptable de activos, describiendo acciones permitidas y prohibidas en el uso de los activos.

Las personas que utilizan los activos deben estar conscientes de estas reglas como parte de su descripción del puesto.

Custodio del activo de Información

Es el encargado de administrar y hacer efectivo los controles de seguridad (toma de copias de seguridad, asignar privilegios de acceso, modificaciones, borrado) que el propietario haya definido.

Las mejores prácticas recomiendan la realización de un inventario y la clasificación de los activos de información de las organizaciones de un inventario para determinar cómo deben ser utilizados, los roles y las responsabilidades que tiene el personal sobre la misma, reconociendo adicionalmente los niveles de confidencialidad que a cada activo deben dársele.

Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes para la organización.

Los activos importantes deben identificarse con claridad, como ya se explicó y posteriormente deben ser tasados para visualizar su impacto en la empresa por su deterioro o por sus fallas en confidencialidad, integridad y disponibilidad, este estudio está enfocado únicamente a la confidencialidad.

Tasación de los activos

La escala de tasación es aquella que ayudó con la valoración de los activos. Cada activo se tasó utilizando una escala de Likert. El valor 1 significa despreciable y 5 muy alta. La pregunta que debe realizarse para utilizar la escala es ¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?

La escala de tasación utilizada:

1 = Despreciable

2 = Baja

3 = Media

4 = Alta

5 = Muy alta

Adicionalmente, la escala de tasación ayuda a calificar a los activos en función del valor o la importancia que tiene el activo para la organización.

Recuerde que la tasación de los activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarque el alcance del modelo.

La información debe clasificarse en función de su valor, sensibilidad y criticidad para la organización.

Niveles de Clasificación

- Pública
- Confidencial

Pública: en Unifinsa la información pública es aquella que ha sido declarada de conocimiento público esta información puede ser entregada o publicada sin restricciones a los colaboradores o a cualquier persona sin que esto implique ningún daño.

Confidencial: la información confidencial de Unifinsa es toda aquella información que no es pública, a este tipo de información solo pueden tener acceso los usuarios a los cuales se les han asignado los permisos.

Niveles de confidencialidad

Existen 3 grados de confidencialidad

- Uso Interno
- Restringida
- Altamente Restringida

Uso Interno

Es toda información que es utilizada por el personal de Unifinsa para realizar sus labores y que no puede ser conocida por terceros sin la autorización del propietario de la información. En el caso de ser conocida utilizada o modificada por personas sin la debida autorización impactaría de forma leve a la organización.

Restringida

Información que es utilizada por un solo grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin la debida autorización del propietario de la información. En el caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a la organización.

Altamente restringida

Información que es utilizada por un solo grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización especial de la organización. En el caso de ser conocida, utilizada o modificada por personas sin la debida autorización impactaría de forma grave a la organización.

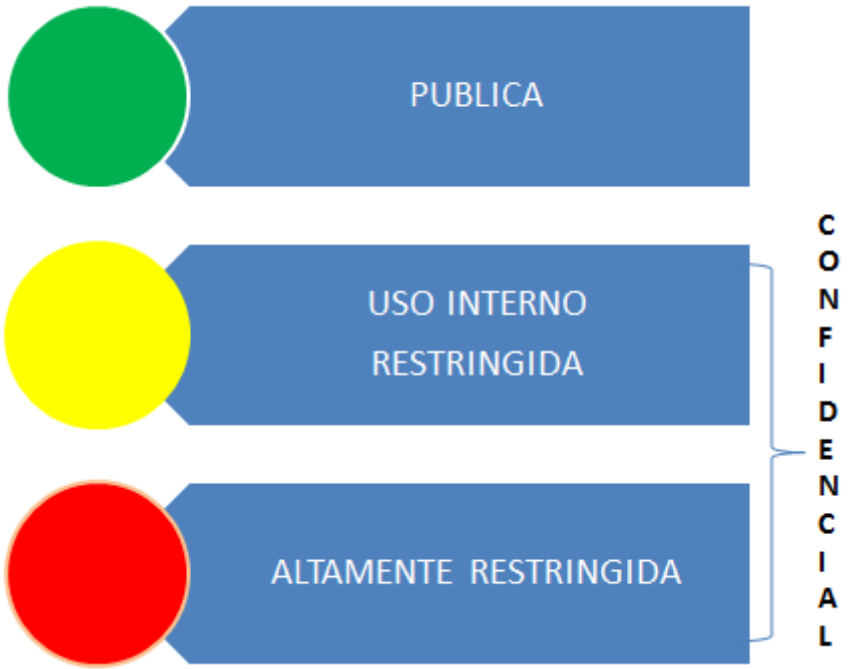


GRAFICO 29. Niveles de clasificación
Elaborado por: LÓPEZ, Mariela (2012)

Análisis y evaluación del riesgo

Metodológicamente para **Alberto G. Alexander (2007: 47-61),** el objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad, y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten causen un incidente.

La organización debe decidir el método para hacer el cálculo del riesgo que sea más apropiado para la empresa y los requerimientos de seguridad.

Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

Amenaza

En la organización, los activos de información están sujetos a distintas formas de amenazas.

Una amenaza puede causar un incidente no deseado que puede causar daño a la organización y a sus activos.

“Una amenaza es la indicación de un potencial evento no deseado” (Alberts y Dorofee, 2003). En esta definición, los autores se refieren a una

situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural.

En conclusión se puede decir que una amenaza es una indicación de un evento no deseado con el potencial de causar daño.

Clasificación de las amenazas

Amenazas naturales: Inundaciones tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.

Amenazas a instalaciones: Fuego, explosión caída de energía, daño de agua, perdida de acceso, fallas mecánicas.

Amenazas Humanas: Huelgas epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave.

Amenazas operacionales: crisis financiera, pérdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad.

Amenazas sociales: motines, protestas, sabotaje, vandalismo bombas, violencia laboral, terrorismo.

Las amenazas se pueden originar de fuentes o eventos accidentales o deliberados.

Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño.

Una vez identificadas las amenazas que pueden afectar un activo de información, se debe evaluar su posibilidad de ocurrencia de una amenaza debe hacerse con un grupo experto que tenga conocimiento de la naturaleza de la amenaza.

Por cada amenaza, para medir la posibilidad de su ocurrencia se recomienda utilizar una escala de Likert donde:

1 = Muy Bajo

2 = Bajo

3 = Medio

4 = Alto

5 = Muy Alto

Las empresas deben tomar decisiones importantes en relación con el análisis de la amenazas. La decisión sobre cuáles amenazas se descartan por tener una ocurrencia baja, debe revisarse con detenimiento.

Una amenaza con baja posibilidad de ocurrencia pudiera tener severas consecuencias económicas en la organización.

Salvaguardas

Las salvaguardas son los controles de seguridad existentes en la organización frente a la amenaza identificada.

Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

Es una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puedes ser explotada para violar la integridad del sistema" (Peltier, 2001).

"Las vulnerabilidades organizacionales son debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas" (Albert y Dorofee, 2003).

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño.
Las vulnerabilidades por las distintas fuentes que las pueden originar se clasifican en:

Control de acceso

Seguridad física y ambiental

Gestión de operaciones y comunicación

Mantenimiento, desarrollo y adquisición de sistemas de información

Gestión de operaciones y comunicaciones

Descripción de las categorías de vulnerabilidades

Las vulnerabilidades pueden clasificarse como:

Seguridad de los recursos humanos

Falta de entrenamiento en seguridad

Carencia de toma de conciencia en seguridad

Falta de mecanismos de monitoreo

Falta de políticas para el uso correcto de las telecomunicaciones

No eliminar los accesos al término del contrato de trabajo

Carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo

Empleados desmotivados

Control de acceso

Segregación inapropiada de redes

Falta de política sobre escritorio y pantalla limpia

Falta de protección al equipo de comunicación móvil

Política incorrecta para el control de acceso

Passwords sin modificarse

Seguridad física y ambiental

Control de acceso físico inadecuado a oficinas salones y edificios en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos

Mal cuidado de los equipos

Gestión de Operaciones y Comunicaciones

Complicadas interfaces para usuarios

Control de cambio inadecuado

Gestión de red inadecuada

Carencia de mecanismos que aseguren el envío y recepción de mensajes

Carencia de tareas segregadas

Carencia de control de copiado

Falta de protección en redes públicas de conexión

Mantenimiento desarrollo y adquisición de sistemas de información

Protección inapropiada de llaves criptográficas

Políticas incompletas para el uso de criptografía

Carencia de validación de datos procesados

Carencia de ensayos de software

Documentación pobre de software

Mala selección de ensayos de datos

Una vez identificadas las vulnerabilidades, por cada una de ellas se debe evaluar la posibilidad de que sean explotadas por la amenaza.

Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre amenazas y vulnerabilidades.

La pregunta fundamental es: ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades?

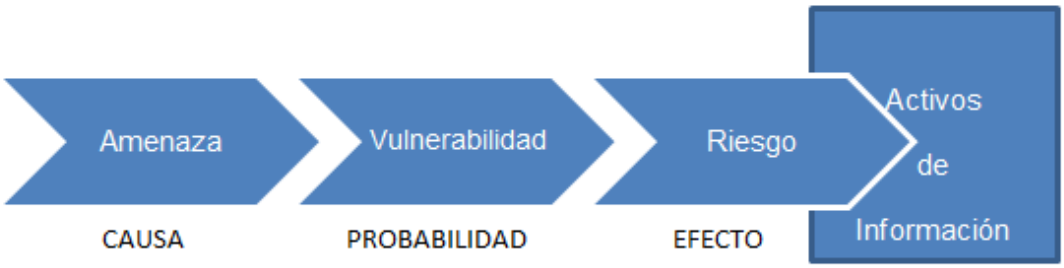


GRAFICO 30. Relación causa-efecto entre elementos del análisis del riesgo
Elaborado por: LÓPEZ, Mariela (2012)

Existe una interdependencia de ellos bajo una relación de causa efecto.

Está muy claro identificar que la variable que la empresa puede manipular y fortalecer, para minimizar que se ponga de manifiesto el riesgo y proteger los activos de información de una penetración de la amenaza, son las vulnerabilidades.

Probabilidad de ocurrencia de la amenaza

Se puede entender como qué tan fácil puede ser explotada las vulnerabilidades por las amenazas.

Se tiene la siguiente escala:

1 = Muy Bajo

2 = Bajo

3 = Medio

4 = Alto

5 = Muy Alto

Valoración del nivel de riesgo

Es el producto del valor del impacto del activo por la probabilidad de ocurrencia de la amenaza.

Evaluación del riesgo

Una vez efectuado el cálculo del riesgo por cada activo, en relación con su amenaza, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos.

Identificar y evaluar las opciones para el tratamiento del riesgo

Reducción del riesgo

Para todas aquello riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos al nivel que se haya definido como aceptable. Es importante mencionar que al hacer identificado el nivel de control, conviene considerar los requerimientos de seguridad relacionados con los riesgos.

Los controles pueden reducir el riesgo estimado en dos maneras:

-Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza.

-Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados reaccionando y recuperándose de ellos.

Para proteger sus activos, una organización escoge adoptar cuál de estas maneras o una combinación de ambas; esta es una decisión comercial

que depende de los requerimientos del negocio, el ambiente y las circunstancias en las cuales la organización necesita operar.

El proceso de selección envuelve numerosas decisiones y consultas y usualmente discusiones con distintas partes de la organización y con un determinado número de personas clave. El proceso de selección requiere producir un resultado que más se adecue a la organización en términos de sus requerimientos para la protección de sus activos, inversiones cultura y tolerancia al riesgo.

Objetivamente aceptar el riesgo

Muchas veces se presenta la situación en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada. Cuando las empresas toman estas decisiones, deben documentarse y definir con precisión el criterio de aceptación del riesgo.

Transferencia del riesgo

La transferencia del riesgo es una opción cuando para la compañía es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.

Existe una serie de mecanismos para transferir los riesgos a otra organización por ejemplo utilizar una aseguradora.

Se requiere analizar la transferencia del riesgo a la aseguradora para identificar cuanto del riesgo actual se transferirá. De modo usual, las empresas aseguradoras no mitigan los impactos no financieros y tampoco proveen mitigación inmediata en el evento de un accidente.

Algo muy importante que debe recordar es el riesgo residual que siempre estará presente.

Por último la responsabilidad por la seguridad de la información y por las instalaciones para el procesamiento de información, al haberse tercerizado estas, siempre le corresponde a la organización original.

Siempre al tercerizar, puede creerse que la empresa prestadora de servicios debe estimar y gestionar nuevos riesgos.

Evitar el riesgo

Por el modo de evitar el riesgo se entiende cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular, para así evitar la presencia del riesgo.
El riesgo puede evitarse por medio de:

-No desarrollar ciertas actividades comerciales

-Mover los activos de un área de riesgo

-Decidir no procesar información particularmente sensitiva

El hecho de evitar el riesgo debe sopesarse contra necesidades financieras y comerciales.

Pudiera ser que se concluya que esta decisión de evitar el riesgo no es factible.

Riesgo Residual

Después de implementar de implementar las decisiones relacionadas con el tratamiento de un riesgo, siempre habrá un remanente de ese mismo riesgo. Justamente el riesgo que queda, después de implantar el plan de tratamiento, se denomina riesgo residual, que puede ser difícil de calcular pero por lo menos debe realizarse una evaluación para asegurar que logra la protección suficiente.

Si el riesgo residual se considera inaceptable, deben tomarse decisiones para resolver su caso. Una opción es identificar diferentes opciones de tratamiento de riesgo; otra es instaurar más controles, o hacer arreglos con aseguradoras para reducir finalmente el riesgo a niveles aceptable.

A veces, dada la naturaleza de la industria y de los riesgos inherentes, reducir los riegos a un nivel aceptable pudiera no ser posible o financieramente aceptable.

Todos los riesgos residuales que se hayan aceptado debieran ser documentados y aprobados por la gerencia.

Objetivos de control y controles para el tratamiento de riesgos

Una vez realizado el proceso de identificar las opciones de tratamiento del riesgo y haber evaluado, la empresa debe decidir cuáles objetivos de control y controles escoger para el tratamiento del riesgo.
La selección de objetivos de control y controles debe efectuarse tomando en cuenta el criterio establecido para la aceptación de los riesgos.

La selección de objetivos de control y controles, según la norma ISO 27001:2005, debe hacerse del Anexo A, el mismo que no se anexó, ya que la norma oficial ISO 27001:2005 (*International Standard Organization* por sus siglas en inglés), que contiene dicho anexo debe adquirirse en las entidades autorizadas para su venta, también se pueden seleccionar objetivos de control y controles adicionales. El anexo debe verse como un punto de inicio de búsqueda de controles.

Plan de tratamiento del riesgo

Una vez que se han tomado las decisiones relacionadas con el tratamiento del riesgo, las actividades para poder implementar estas decisiones tienen que ejecutarse. Para este fin hay que identificar y planear las actividades. Cada actividad de implementación debe ser identificada con claridad y desagregarse un una gama de subactividades requeridas para poder distribuir las responsabilidades a las personas, estimar los requerimientos de recursos, el conjunto de entregables, las fechas críticas y la supervisión del progreso.

Una vez formulado el plan de tratamiento del riesgo, se deben asignar los recursos y las acciones correspondientes para implementar las decisiones de la gestión del riesgo que deben iniciarse.

6.7. Metodología. Modelo Operativo

TABLA 31. Modelo Operativo

FASES	ETAPAS	METAS	ACTIVIDADES	RECURSOS	RESPONSABLE	FECHA DE CUMPLIMIENTO
INICIAL	Valoración de Activos de Información	Identificar y Valorar los Activos de Información importantes para la organización	• Identificar los activos críticos • Valorar los activos	Equipo multidisciplinario, Materiales de oficina, Computador	Oficial de Seguridad de la Información	Septiembre y Octubre 2012
MEDIA	Análisis y evaluación de riesgos de los activos de información	Análizar y Evaluar los Riesgos de los Activos de Información	• Identificar los activos que tiene mayor riesgo para la organización • Identificar la amenazas • Identificar las salvaguarda • Identificar las vulnerabilidades • Evaluar la probabilidad de que se efectivice las amenazas • Identificar el nivel de riesgo	Equipo multidisciplinario, Materiales de oficina, Computador	Oficial de Seguridad de la Información	Noviembre y Diciembre 2012
FINAL	Selección de controles	Identificar y evaluar controles adecuados	• Seleccionar el tipo de tratamiento del riesgo • Establecer los controles (Anexo A Norma ISO 27000:2005)	Equipo multidisciplinario, Materiales de oficina, Computador	Oficial de Seguridad de la Información	Diciembre 2012
	Plan de tratamiento de riesgo	Elaborar el plan de tratamiento de riesgo	• Elaborar el plan de tratamiento de riesgo definiendo: - Actividades - Plazos - Responsables - Recursos	Equipo multidisciplinario, Materiales de oficina, Computador	Oficial de Seguridad de la Información	Enero y Agosto 2013

Fuente: ISO 27001:2005 (*International Standard Organization* por sus siglas en inglés)

Elaborado por: LÓPEZ, Mariela (2012)

La metodología consta de las siguientes fases:

6.7.1 Fase Inicial

6.7.1.1 Valoración de los activos de Información

Se identificaron los activos de información de la organización, que son aquellos que tienen valor para la institución. Debido a que la información es confidencial, nos referiremos con un código 01, 02, 03, etc. al nombre del activo de información.

En base al activo de información, se identificó el tipo de activo tomando en cuenta la siguiente clasificación:

-Activos de información (datos, manuales de usuario, etc.)

-Documentos de papel (contratos)

-Activos de Software (Aplicación, software de sistemas, etc.)

-Activos Físicos (computadoras, medios magnéticos, etc.)

-Personal (Cliente, personal)

-Imagen de la compañía y reputación

-Servicios (comunicaciones, etc.)

Es importante identificar al propietario del activo información

Se identificó quien custodia el activo de información

La información debe clasificarse en función de su valor, criticidad y sensibilidad para la organización, para el efecto utilizamos:

La escala de tasación:

1 = Despreciable

2 = Baja

3 = Media

4 = Alta

5 = Muy alta

La escala de tasación ayuda a calificar a los activos en función del valor o la importancia que tiene el activo para la organización.

Para identificar la criticidad, la pregunta que debe realizarse para utilizar la escala es ¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?

Se definió el valor del impacto del activo bajo el siguiente criterio:

$$\frac{Importancia + Confidencialidad + Integridad + Disponibilidad}{4}$$

Se identificó la sensibilidad de los activos de información de acuerdo a los niveles de clasificación:

Pública

Confidencial:
-Uso Interno
-Restringida
-Altamente Restringida

Se ordenó de mayor a menor la columna “valor del impacto del activo”, siendo la Administración quien decide desde que rango se va a considerar activos críticos, y activos no críticos.

En este caso de estudio se denominó activos críticos a aquellos valores que estuvieron entre el 3 y 5, mientras que a los activos que estuvieron entre 1 y 2.99 se denominaron activos no críticos, sobre los cuales no se realizó ninguna evaluación.

6.7.2 Fase Media

6.7.2.1 Análisis y evaluación de riesgos de los activos de información

Se enlistaron los Activos Críticos junto con el “valor del impacto del activo”.

Se identificó el tipo de Amenaza, junto con las amenazas a las que están expuestos los activos.

Se Identificaron las salvaguardas y las vulnerabilidades.

Se evaluó la probabilidad de que se efectivicen las amenazas considerando las salvaguardas y las vulnerabilidades existentes.

Se utilizó la siguiente escala:

1 = Muy Bajo

2 = Bajo

3 = Medio

4 = Alto

5 = Muy Alto

Valoración del nivel de riesgo.- Es el producto del valor del impacto del activo por la probabilidad de ocurrencia de la amenaza.

Evaluación del riesgo.- Ayuda a identificar los niveles de riesgo, es importante que los rangos sean establecidos por la Administración, debiendo estar documentados formalmente, en este caso se consideró lo siguiente:

TABLA 32. Evaluación del riesgo

	Valoración del nivel de riesgo	Evaluación del riesgo
Riesgo Bajo	1 a 10	ACEPTABLES
Riesgo Medio	10,1 a 15	NO ACEPTABLES
Riesgo Alto	15,1 a 25	NO ACEPTABLES

Fuente: Unifinsa Elaborado por: LÓPEZ, Mariela (2012)

Los riesgos que serán evaluados en el plan de tratamiento de riesgo, son los riesgos medio y riesgo alto, a los cuales se los consideró como “NO ACEPTABLES”.

6.7.3 Fase Final

6.7.3.1 Seleccionar objetivos de control y controles para el tratamiento de riesgos.

Se enlistó los activos de información, junto con la amenaza, identificando el tipo de amenaza, las salvaguardas existentes y cada una de las vulnerabilidades a las que la institución está expuesta.

Identificar y evaluar las opciones para el tratamiento del riesgo

Entre las opciones de tratamiento se tiene:

-Reducción del riesgo

Los controles pueden reducir el riesgo estimado en dos maneras:

Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza.

Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados reaccionando y recuperándose de ellos.

-Objetivamente aceptar el riesgo

-Transferencia del riesgo

-Evitar el riesgo

Se Identificó si existen Asuntos legales relacionados al momento de seleccionar los controles.

Decidir que controles seleccionar para el tratamiento del riesgo; para lo cual se utilizó el Anexo A de la ISO 27001:2005, que es propiedad de Unifinsa, el mismo que no se anexó, ya que la norma oficial de la ISO 27001:2005 (*International Standard Organization* por sus siglas en inglés), que contiene dicho anexo, debe adquirirse en las entidades autorizadas para su venta.

Es importante recordar, que este estudio estuvo enfocado a mitigar los riegos de pérdida de confidencialidad.

6.7.3.2 Plan de tratamiento del riesgo

Se elaboró un plan de tratamiento con todos los activos no tolerables, estableciendo:

Se definió la actividad o conjunto de actividades que me ayudaran a controlar el riesgo.

Se indicó los recursos necesarios para el correcto desarrollo de la actividad y los plazos de cumplimiento.

Es muy importante la definición de un responsable para el correcto desenvolvimiento de la actividad.

TABLA 33. Matriz de levantamiento de activos de información

Matriz de levantamiento de activos de información										
Objetivo: Levantar la información para contar con un inventario de los activos de información que tienen valor para la organización										
Fecha: 03/09/2012					Proceso: Crédito					
Colaborador Entrevistado1		Nombre: Confidencial			Cargo: Jefe de Credito					
No Activo	**Nombre del Activo**	**tipo de activo**	**Propietario**	**Custodio**	**valor**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor del impact**	**Clasificación**
1	01	Información	Jefe de Crédito	Adm Base Datos	5	5	5	5	5	Uso Interno
2	02	Software	Jefe de Crédito	Adm Aplicaciones	5	5	5	5	5	Uso Interno
3	03	Información	Jefe de Crédito	Jefe de credito	5	5	3	4	4,25	Restringido
4	04	Documento	Jefe de Captaciones	Adm de Archivo	5	4	4	4	4,25	Restringido
5	05	Información	Jefe de Crédito	Adm de Cobranzas	3	3	5	5	4	Restringido
6	06	Información	usuario	usuario	4	4	3	4	3,75	Restringido
7	07	Documento	Jefe de Crédito	Adm de Archivo	3	3	3	5	3,5	Uso Interno
8	08	Documento	Jefe de Captaciones	Captaciones	3	4	5	2	3,5	Restringido
9	09	Información	Jefe de Crédito	CGTH	3	3	4	3	3,25	Uso Interno
10	010	Información	Jefe de Crédito	CGTH	3	3	4	3	3,25	Restringido
11	011	Información	usuario	usuario	3	3	3	3	3	Altamente Restringido
12	012	Información	usuario	usuario	3	3	3	3	3	Altamente Restringido
13	013	Información	Jefe de Captaciones	Adm de Archivo	3	2	3	3	2,75	Restringido
14	014	Información	Jefe de Crédito	Adm Active Directory	2,5	2	3	2	2,375	Restringido
15	015	Información	Jefe de Captaciones	Adm de Archivo	2	2	2	3	2,25	Restringido

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 34. Matriz de análisis y evaluación de riesgo

Análisis y Evaluación de Riesgos

Objetivo:	Identificar los activos que tienen mayor riesgo de pérdida de confidencialidad				
Fecha:	04/09/2012		Proceso:		Crédito
Colaborador Entrevistado1	Nombre:	confidencial		Cargo:	Jefe de Crédito
Colaborador Entrevistado2	Nombre:	confidencial		Cargo:	Oficial de Seguridad

Nº.	ACTIVOS CRITICOS	VALOR DEL IMPACTO DEL ACTIVO	TIPO	AMENAZA	SALVAGUARDAS ACTUALES	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	VALORACION DEL NIVEL DE RIESGOS	EVALUACION DEL RIESGO
1	01	5	Humanas	fuga de información	Unicamente los usuarios autorizados cuentan con correo electrónico externo Empleados nuevos reciben capacitación en seguridad de la Información	La institución no cuenta con una herramienta que alerte la salida de información confidencial No existe un clasificación de la información respecto a la sensibilidad de la información Falta de concientización a los usuarios del correcto tratamiento de la información	4	20	NO ACEPTABLE
			Humanas	Acceso no autorizados	Permisos por Roles	• Falta de mecanismos de monitoreo • No eliminar los accesos al término del contrato de trabajo o por cambio de cargo • Política incorrecta para el control de acceso	3	15	NO ACEPTABLE
			Humanas	Robo de equipos portátiles	N/A	La información no está encriptada	3	15	NO ACEPTABLE

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 34a. Matriz de análisis y evaluación de riesgo

Análisis y Evaluación de Riesgos									
Objetivo:	Identificar los activos que tienen mayor riesgo de pérdida de confidencialidad								
Fecha:	04/09/2012				Proceso:	Crédito			
Colaborador Entrevistado1	Nombre:	confidencial			Cargo:	Jefe de Crédito			
Colaborador Entrevistado2	Nombre:	confidencial			Cargo:	Oficial de Seguridad			
Nº.	**ACTIVOS CRITICOS**	**VALOR DEL IMPACTO DEL ACTIVO**	**TIPO**	**AMENAZA**	**SALVAGUARDAS ACTUALES**	**VULNERABILIDAD**	**PROBABILIDAD DE OCURRENCIA DE LA AMENAZA**	**VALORACION DEL NIVEL DE RIESGOS**	**EVALUACION DEL RIESGO**
2	02	5	Humanas	Acceso no autorizados	cuentas de usuario Roles	Falta de mecanismos de monitoreo para detectar accesos no autorizados • Falta levantamiento de los accesos al sistema transaccional.	3	15	NO ACEPTABLE
3	03	5	Humanas	Acceso no autorizados	N/A	Equipos portátiles poseen acceso a los puertos USB No existe un clasificación de la información respecto a la sensibilidad de la información	2	10	NO ACEPTABLE
5	05	4,0	Humanas	Pérdida de confidencialidad	Roles Claves de Accesos	Falta depuración de roles de acceso	3	12	NO ACEPTABLE
			Humanas	incertidumbre en la organización	Roles Carpetas compartidas restringidas	Usuarios no autorizados tengan acceso a la infromación Falta realizar un levantamiento de las carpetas compartidas y los accesos de cada uno de los usuarios a las mismas	4	16	NO ACEPTABLE

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 34b. Matriz de análisis y evaluación de riesgo

Análisis y Evaluación de Riesgos									
Objetivo:	Identificar los activos que tienen mayor riesgo de pérdida de confidencialidad								
Fecha:	04/09/2012				Proceso:	Crédito			
Colaborador Entrevistado1	Nombre:	confidencial			Cargo:	Jefe de Crédito			
Colaborador Entrevistado2	Nombre:	confidencial			Cargo:	Oficial de Seguridad			

Nº.	ACTIVOS CRITICOS	VALOR DEL IMPACTO DEL ACTIVO	TIPO	AMENAZA	SALVAGUARDAS ACTUALES	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	VALORACION DEL NIVEL DE RIESGOS	EVALUACION DEL RIESGO
6	06	3,8	Sociales	Robo de equipos portátiles	Software de respaldo en equipos críticos	La información no está encriptada	3	11,25	NO ACEPTABLE
10	010	3,3	Humanas	Pérdida de confidencialidad	Herramienta de control de documentos no pueden ser impresos sin una autorización	Descuido en el manejo de la documentación por parte del usuario. Información es olvidada en los escritorios	4	13	NO ACEPTABLE
13	013	2,8	Humanas	fuga de información	cuentas de usuario	Que los usuarios aprovechen que tiene acceso a la información y consulten información de cualquier persona sin que exista una solicitud de crédito de por medio	4	11	NO ACEPTABLE
14	014	2,4	Humanas	Acceso no autorizado	control de acceso a las carpetas compartidas	Falta depurar las carpetas compartidas no se retiran los permisos cuando existe un cambio de cargo	4	9,48	ACEPTABLE
11	011	3,0	Humanas	fuga de información	Logs de auditoria de Active Directory	Divulgación de claves por parte del personal Falta de difusión de las políticas de seguridad Falta de concientización del personal	5	15	NO ACEPTABLE

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 34c. Matriz de análisis y evaluación de riesgo

Análisis y Evaluación de Riesgos									
Objetivo:	Identificar los activos que tienen mayor riesgo de pérdida de confidencialidad								
Fecha:	04/09/2012					Proceso:	Crédito		
Colaborador Entrevistado1	Nombre:	confidencial				Cargo:	Jefe de Crédito		
Colaborador Entrevistado2	Nombre:	confidencial				Cargo:	Oficial de Seguridad		

CLASIFICACION DE LA INFORMACION			EVALUACION DE AMENAZAS					VALORACION DEL RIESGO	
Nº.	ACTIVOS CRITICOS	VALOR DEL IMPACTO DEL ACTIVO	TIPO	AMENAZA	SALVAGUARDAS ACTUALES	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	VALORACION DEL NIVEL DE RIESGOS	EVALUACION DEL RIESGO
12	012	3,0	Humanas	fuga de información	generación automática de contraseñas provisionales. Logs de auditoría del Sistema Transaccional	Divulgación de claves por parte del personal Falta de difusión de las políticas de seguridad Falta de concientización del personal	4	12	NO ACEPTABLE
7	07	3,5	Humanas	Pérdida de Carpeta	Archivo Bitácora de entrega de Carpetas	Error en el manejo de entrada y salida de documentos	4	14	NO ACEPTABLE

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 34d. Matriz de análisis y evaluación de riesgo

Análisis y Evaluación de Riesgos									
Objetivo:	Identificar los activos que tienen mayor riesgo de pérdida de confidencialidad								
Fecha:	04/09/2012					Proceso:	Crédito		
Colaborador Entrevistado1	Nombre:	confidencial				Cargo:	Jefe de Crédito		
Colaborador Entrevistado2	Nombre:	confidencial				Cargo:	Oficial de Seguridad		

CLASIFICACION DE LA INFORMACION			EVALUACION DE AMENAZAS					VALORACION DEL RIESGO	
Nº.	ACTIVOS CRITICOS	VALOR DEL IMPACTO DEL ACTIVO	TIPO	AMENAZA	SALVAGUARDAS ACTUALES	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	VALORACION DEL NIVEL DE RIESGOS	EVALUACION DEL RIESGO
4	04	3,58	Humanas	Pérdida o destrucción del documento	PECs Información del Buro Acta de comité física Revisión del Comité de Crédito Sfinge Administración adecuada del archivo de crédito	Error en el manejo de entrada y salida de documentos Error de ingreso de la información a Sfinge	2	7,17	ACEPTABLE
			Física	Acceso indebido a los documentos	Acceso controlado con tarjetas magnéticas. Personal responsable que custodian los documentos. Bitácoras de control de salida/ingreso de documentos	Descuido en el manejo de tarjetas de acceso. Falta de actualización de roles y permisos de tarjetas magnéticas cuando son cambiadas de áreas o personas temporales o promovidas.	2	7,17	ACEPTABLE

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 34e. Matriz de análisis y evaluación de riesgo

Análisis y Evaluación de Riesgos				
Objetivo:	Identificar los activos que tienen mayor riesgo de pérdida de confidencialidad			
Fecha:	04/09/2012		Proceso:	Crédito
Colaborador Entrevistado1	Nombre:	confidencial	Cargo:	Jefe de Crédito
Colaborador Entrevistado2	Nombre:	confidencial	Cargo:	Oficial de Seguridad

CLASIFICACION DE LA INFORMACION			EVALUACION DE AMENAZAS					VALORACION DEL RIESGO	
Nº.	ACTIVOS CRITICOS	VALOR DEL IMPACTO DEL ACTIVO	TIPO	AMENAZA	SALVAGUARDAS ACTUALES	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	VALORACION DEL NIVEL DE RIESGOS	EVALUACION DEL RIESGO
8	08	3,50	Humanas	fuga de información	Documento original en custodia Reportes diarios de certificados en custodia Alerta de certificado pignorado en Sfinge	Falta de capacitación referente a la seguridad de la información por cambio de Funciones	3,3	11,55	NO ACEPTABLE
15	015	2,25	Humanas	fuga de información	Cambio de claves de usuarios cada 60 días (alfa-numéricas) Políticas de seguridad Control de acceso automático a las aplicaciones y datos por roles (permisos) Logs de auditoría informática a nivel de transacción	Falta de actualización de roles y permisos de tarjetas magnéticas cuando son cambiadas de áreas o personas temporales o promovidas.	3,5	7,88	ACEPTABLE

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 35. Matriz de controles para el tratamiento de riesgos

Controles para el Tratamiento de Riesgos							
Objetivo:	Definir los controles para aquellos activos de información de riesgo inaceptable						
Fecha:	10/09/2012				Proceso: Crédito		
Colaborador Entrevistado1	Nombre:	Confidencial			Cargo: Jefe de Crédito		
Colaborador Entrevistado2	Nombre:	Confidencial			Cargo: Oficial de Seguridad de la Información		
ACTIVOS	**AMENAZA**	**TIPO DE AMENAZA**	**SALVAGUARDAS ACTUALES**	**VULNERABILIDAD**	**TIPO DE OPCION DE TRATAMIENTO**	**ASUNTOS LEGALES RELACIONADOS**	**CONTROLES**
01	fuga de información	Humanas	Unicamente los usuarios autorizados cuentan con correo electrónico externo Claves de acceso a Sfinge	La institución no cuenta con una herramienta que alerte la salida de información confidencial	Control	Sigilo bancario	A.8.2.2 Concienciación, formación y capacitación A.7.1.3 Uso aceptable de los activos
				No existe un clasificación de la información respecto a la sensibilidad de la información	Control	Sigilo bancario	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manipulado de la información
				Falta de concientización a los usuarios del correcto tratamiento de la información	Control	Sigilo bancario	A.8.1.1 Funciones y responsabilidades A.6.1.5 Acuerdos de confidencialidad A.8.2.2 Concienciación, formación y capacitación A.7.1.3 Uso aceptable de los activos
	Acceso no autorizados	Humana	Permisos por roles	Falta de mecanismos de monitoreo de accesos no autorizados	Control	Sigilo bancario	A.10.10.2 Supervisión del uso del sistema
				No eliminar los accesos al término del contrato de trabajo o por cambio de cargo	Control	Sigilo bancario	A.8.3 Cese del empleo o cambio de puesto de trabajo A.8.3.1 Responsabilidades del cese o cambio A.8.3.3 Retirada de los derechos de acceso A.8.3.2 Devolución de activos
				Política incorrecta para el control de acceso	Control	Sigilo bancario	A.11.2.1 Registro de usuarios A.11.2.2 Gestión de privilegios

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 35a. Matriz de controles para el tratamiento de riesgos

Controles para el Tratamiento de Riesgos							
Objetivo:	Definir los controles para aquellos activos de información de riesgo inaceptable						
Fecha:	10/09/2012				Proceso:		
Colaborador Entrevistado1	Nombre:	Confidencial			Cargo: Jefe de Crédito		
Colaborador Entrevistado2	Nombre:	Confidencial			Cargo: Oficial de Seguridad de la Información		
ACTIVOS	**AMENAZA**	**TIPO DE AMENAZA**	**SALVAGUARDAS ACTUALES**	**VULNERABILIDAD**	**TIPO DE OPCION DE TRATAMIENTO**	**ASUNTOS LEGALES RELACIONADOS**	**CONTROLES**
02	Acceso no autorizados	Humana	cuentas de usuario Roles	Falta de mecanismos de monitoreo para detectar accesos no autorizados	Control		A.10.7.3 Procedimientos de manipulación de la información A.10.10.1 Registro de la auditoria A.10.10.2 Supervisión del uso del sistema
				Falta levantamiento de los accesos al sistema transaccional.	Control		A.11.2.2 Gestión de privilegios A.11.2.4 Revisión de los derechos de acceso de usuarios
05	Pérdida de confidencialidad	Humana	Roles Claves de Accesos	Falta depuración de roles de acceso	Control		A11.6.1 Restricción del acceso a la información
	incertidumbre en la organización	Humana	Roles Carpetas compartidas restringidas	Usuarios no autorizados tengan acceso a la infromación	Control		A.11.1.1 Política de control de acceso
				Falta realizar un levantamiento de las carpetas compartidas y los accesos de cada uno de los usuarios a las mismas	Control		A.11.2.4 Revisión de los derechos de acceso de usuarios

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 35b. Matriz de controles para el tratamiento de riesgos

Controles para el Tratamiento de Riesgos							
Objetivo:	Definir los controles para aquellos activos de información de riesgo inaceptable						
Fecha:	10/09/2012				Proceso:		
Colaborador Entrevistado1	Nombre:	Confidencial			Cargo: Jefe de Crédito		
Colaborador Entrevistado2	Nombre:	Confidencial			Cargo: Oficial de Seguridad de la Información		
ACTIVOS	**AMENAZA**	**TIPO DE AMENAZA**	**SALVAGUARDAS ACTUALES**	**VULNERABILIDAD**	**TIPO DE OPCION DE TRATAMIENTO**	**ASUNTOS LEGALES RELACIONADOS**	**CONTROLES**
06	Robo de equipos portátiles	Humana	Software de respaldo en equipos críticos	La información no está encriptada	Control		A.10.5.1 Copias de seguridad de la información A.9.2.5 Seguridad de equipos fuera de las instalaciones
10	Pérdida de confidencialidad	Humana	Herramienta de control de documentos no pueden ser impresos sin una autorización	Descuido en el manejo de la documentación por parte del usuario. Información es olvidada en los escritorios	Control		A.7.2.2 Etiquetado y manipulado de la información A.6.1.5 Acuerdos de confidencialidad A.11.3.3 Política de puesto de trabajo despejado y pantalla limpia
				No existe un control al momento de usar la fotocopiadores;	Control		A.11.1.1 Política de control de accesos
13	fuga de información	Humana	cuentas de usuario	Que los usuarios aprovechen que tiene acceso a la información y consulten información de cualquier persona sin que exista una solicitud de crédito de por medio	Control	Sigilo bancario	A.11.3 Responsabilidades de usuario A.11.3.1 Uso de contraseñas

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 35c. Matriz de controles para el tratamiento de riesgos

Controles para el Tratamiento de Riesgos							
Objetivo:	Definir los controles para aquellos activos de información de riesgo inaceptable						
Fecha:	10/09/2012				Proceso:		
Colaborador Entrevistado1	Nombre:	Confidencial			Cargo: Jefe de Crédito		
Colaborador Entrevistado2	Nombre:	Confidencial			Cargo: Oficial de Seguridad de la Información		
ACTIVOS	**AMENAZA**	**TIPO DE AMENAZA**	**SALVAGUARDAS ACTUALES**	**VULNERABILIDAD**	**TIPO DE OPCION DE TRATAMIENTO**	**ASUNTOS LEGALES RELACIONADOS**	**CONTROLES**
11	fuga de información	Humana	Logs de auditoria de Active Directory	Divulgación de claves por parte del persona	Control		A.11.3 Responsabilidades de usuario A.11.3.1 Uso de contraseñas
				Falta de difusión de las políticas de seguridad	Control		A.8.2.2 Concienciación, formación y capacitación
				Falta de concientización del personal	Control		A.8.1.1 Funciones y responsabilidades
12	fuga de información	Humana	generación automática de contraseñas provisionales. Logs de auditoría	Divulgación de claves por parte del personal Falta de difusión de las políticas de seguridad Falta de concientización del personal	Control		A.8.2.2 Concienciación, formación y capacitación
07	Pérdida de Carpeta	Humana	Las carpetas son custodiadas en Archivo Bitácora de entrega de Carpetas	Error en el manejo de entrada y salida de documentos	Control		A.9.1.2 Controles físicos de entradas

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 36. Plan de tratamiento de riesgo

Plan de Tratamiento de Riesgos								
Objetivo: Definir el tratamiento de riesgo para aquellos activos de información de riesgo inaceptable								
Fecha: 11/09/2012			Proceso:Crédito					
Colaborador Entrevistado1	Nombre: Confidencial		Cargo: Jefe de Crédito					
Colaborador Entrevistado2	Nombre: Confidencial		Cargo: Oficial de Seguridad de la Información					
Nº.	**PROCESO**	**ACTIVIDAD**	**CONTROL**	**ACTIVO**	**RECURSOS**	**PRESUPUESTO USD**	**FECHA FIN**	**RESPONSABLE**
1	**CREDITO**	Elaborar un programa de capacitación al personal en seguridad de la información Capacitación en seguridad de la Información	A.8.2.2 Concienciación, formación y capacitación	01	Apoyo de consultor, Económicos	5000	31/10/2012	Oficial de Seguridad de la Información
		Elaborar políticas para el uso aceptable de los activos de información	A.7.1.3 Uso aceptable de los activos		tiempo, equipo	N/A	31/10/2012	
		Definir un proceso de Clasificación de la información respecto a la sensibilidad de la información	A.7.2.1 Directrices de clasificación		Apoyo de consultor, Económicos	7000	30/11/2012	
		Difinir técnicas de marcado para identificar el tipos de información	A.7.2.2 Etiquetado y manipulado de la información		Apoyo de consultor, Económicos		30/11/2012	
		Definir responsabilidades de seguridad de la información dentro de la funciones laborales	A.8.1.1 Funciones y responsabilidades		equipo	N/A	30/11/2012	Oficial de Seguridad de la Información
		Elaborar un formato de compromiso de confidencialidad como condición inicial de empleo para funcionarios de crédito Establecer compromisos de confidencialidad con todo el personal y usuarios externos a las instalaciones de procesamiento de información	A.6.1.5 Acuerdos de confidencialidad		equipo	N/A	30/11/2013	Gestion de Talento Humano
		Identificar herramientas que permitan revisar logs de auditoría	A.10.10.2 Supervisión del uso del sistema		software, equipo, licencias por equipo	5000	31/10/2012	Oficial de Seguridad de la Información
		Definir procedimiento para la eliminación segura de derechos de acceso, medios de información hasta la culminación del empleo, o cambio de cargo	A.8.3 Cese del empleo o cambio de puesto de trabajo A.8.3.1 Responsabilidades del cese o cambio A.8.3.3 Retirada de los derechos de acceso A.8.3.2 Devolución de activos		equipo	N/A	30/12/2012	Oficial de Seguridad de la Información
		Elaborar un procedimiento de altas y bajas de usuario a los sistemas y servicios de información	A.11.2.1 Registro de usuarios		equipo	N/A	30/12/2012	Oficial de Seguridad de la Información
		Elaborar un procedimiento que controle el uso y la asignación de privilegios	A.11.2.2 Gestión de privilegios		equipo	N/A	30/12/2012	Oficial de Seguridad de la Información

Fuente: Unifinsa Elaborado por: LÓPEZ, Mariela (2012)

TABLA 36a. Plan de tratamiento de riesgo

Plan de Tratamiento de Riesgos								
Objetivo: Definir el tratamiento de riesgo para aquellos activos de información de riesgo inaceptable								
Fecha: 11/09/2012			Proceso:Crédito					
Colaborador Entrevistado1	Nombre: Confidencial		Cargo: Jefe de Crédito					
Colaborador Entrevistado2	Nombre: Confidencial		Cargo: Oficial de Seguridad de la Información					
Nº.	**PROCESO**	**ACTIVIDAD**	**CONTROL**	**ACTIVO**	**RECURSOS**	**PRESUPUESTO USD**	**FECHA FIN**	**RESPONSABLE**
2	**CREDITO**	Elaborar una política de control de acceso al sistema transaccional. Definir perfiles de acceso de usuarios estandar	A.10.7.3 Procedimientos de manipulación de la información	02	equipo	N/A	30/03/2013	Oficial de Seguridad de la Información
		Contar con una herramienta que permita revisar los logs de auditoría. Definir un proceso de revisión de logs de auditoría	A.10.10.1 Registro de la auditoria		equipo	N/A	30/03/2013	Oficial de Seguridad de la Información
		Implementar procedimientos para el control y la asignación de accesos a los sistemas de datos y servicios de información	A.10.10.2 Supervisión del uso del sistema		equipo	N/A	30/03/2013	Responsable de RRHH
		Elaborar un procedimiento que controle el uso y la asignación de privilegios al sistema transaccional	A.11.2.2 Gestión de privilegios		equipo	N/A	30/04/2013	Oficial de Seguridad de la Información
		Elaborar bitácora de los privilegios asignados por roles de usuario Depuración de los accesos al sistema Transaccional	A.11.2.4 Revisión de los derechos de acceso de usuarios		equipo	N/A	30/04/2013	Oficial de Seguridad de la Información
5	**CREDITO**	Elaborar bitácora de los privilegios asignados a los usuarios de Crédito	A11.6.1 Restricción del acceso a la información	05	equipo	N/A	30/04/2013	Oficial de Seguridad de la Información
		Elaborar una política de control de acceso al sistema transaccional.	A.11.1.1 Política de control de accesos		equipo	N/A	30/04/2013	Oficial de Seguridad de la Información
		Elaborar una política de revisión periódica de los derechos de acceso de los usuarios al sistema transaccional	A.11.2.4 Revisión de los derechos de acceso de usuarios		equipo	N/A	30/04/2013	Oficial de Seguridad de la Información
6	**CREDITO**	Definir equipos críticos (equipos de usuarios) Establecer un mecanismo de respaldo de equipos con información crítica verificar que tan efectivo es el mecanismo de respaldo seleccionado	A.10.5.1 Copias de seguridad de la información	06	tiempo, equipo, software, licencia	25000	30/05/2013	Oficial de Seguridad de la Información
		Definir politicas de entrada y salida de equipos portátiles	A.9.2.5 Seguridad de equipos fuera de las instalaciones		equipo	N/A	28/02/2012	

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

TABLA 36b. Plan de tratamiento de riesgo

Plan de Tratamiento de Riesgos								
Objetivo: Definir el tratamiento de riesgo para aquellos activos de información de riesgo inaceptable								
Fecha: 11/09/2012			Proceso:Crédito					
Colaborador Entrevistado1	Nombre: Confidencial		Cargo: Jefe de Crédito					
Colaborador Entrevistado2	Nombre: Confidencial		Cargo: Oficial de Seguridad de la Información					
Nº.	**PROCESO**	**ACTIVIDAD**	**CONTROL**	**ACTIVO**	**RECURSOS**	**PRESUPUESTO USD**	**FECHA FIN**	**RESPONSABLE**
10	**CREDITO**	Difinir técnicas de marcado para identificar el tipos de información sensible del negocio	A.7.2.2 Etiquetado y manipulado de la información	010	equipo	N/A	30/05/2013	Oficial de Seguridad de la Información
		Definir períodos de revisión de los acuerdos de confidencialidad firmados por el personal fijo y temporal	A.6.1.5 Acuerdos de confidencialidad		equipo	N/A	30/05/2013	Oficial de Seguridad de la Información
		Definir políticas de Mesa Limpia Campaña de Políticas de Mesa limpia incentivando a todo el personal	A.11.3.3 Política de puesto de trabajo despejado y pantalla limpia		Campaña, afiches, carteles	5000	30/05/2013	Oficial de Seguridad de la Información
13	**CREDITO**	Definir Políticas de uso de contraseñas	A.11.3 Responsabilidades de usuario A.11.3.1 Uso de contraseñas	013	equipo	N/A	30/06/2013	Oficial de Seguridad de la Información
11	**CREDITO**	Capacitar a los empleados sobre las políticas de las contraseñas y como crear contraseñas seguras Explicar las efectos de compartir claves de windows	A.11.3 Responsabilidades de usuario A.11.3.1 Uso de contraseñas	011	Apoyo de consultor, Económicos	10000	30/06/2013	Oficial de Seguridad de la Información
		Campaña de uso correcto de contraseñas	A.8.2.2 Concienciación, formación y capacitación		Campaña, afiches, carteles	3000	30/06/2013	Oficial de Seguridad de la Información
		Incluir en la inducción de seguridad de la información las reponsabilidades del buen uso de la contraseñas de active directory	A.8.1.1 Funciones y responsabilidades		tiempo, equipo	N/A	30/06/2013	Oficial de Seguridad de la Información
12	**CREDITO**	Capacitar a los empleados sobre las políticas de las contraseñas y como crear contraseñas seguras Explicar las efectos de compartir claves del sistema tranaccional	A.8.2.2 Concienciación, formación y capacitación	012	Campaña, afiches, carteles	2000	30/06/2013	Oficial de Seguridad de la Información
7	**CREDITO**	Definir una política de acceso para el área de Archivo	A.9.1.2 Controles físicos de entradas	07	equipo	N/A	28/07/2013	Jefe de Captaciones
		Incluir en la política de mesa limpia aspectos de horarios: horas de almuerzo y horas no laborables	A.11.3.3 Política de puesto de trabajo despejado y pantalla limpia		equipo, campaña	2000	28/07/2013	Coordinador de Proyectos
TOTAL PRESUPUESTO						64.000,00		

Fuente: Unifinsa

Elaborado por: LÓPEZ, Mariela (2012)

6.8. Administración

La administración de la presente propuesta deberá estar a cargo del Oficial de seguridad de la Información, con el apoyo de las Jefaturas, el Oficial de seguridad de la información quién tiene la responsabilidad de poner en marcha el proyecto, motivando al personal para que se cumpla a cabalidad lo planteado. Además de dar el seguimiento adecuado a la ejecución del proyecto.

6.9. Previsión de la evaluación

Evaluación Ex Ante

Se deberá evaluar durante el desarrollo y ejecución de la presente propuesta. Es necesario evaluar para conocer y analizar que etapas se han cumplido y al final conocer los resultados realmente obtenidos.

Evaluación Concurrente o en proceso

Para posibilitar cambios a través de la retroalimentación, se debe evaluar la propuesta durante su desarrollo, esta revisión será mensual durante el 1er año, para hacer seguimiento progresivo de cómo se está desarrollando el plan de tratamiento de riesgo, y para que el nivel correspondiente tome acciones.

Evaluación Expost o final

Al término del primer año de gestión, se debe efectuar una evaluación final, con el propósito de conocer los resultados.

Estas evaluaciones estarán a cargo del Oficial de Seguridad de la Información, quién deberá emitir el informe correspondiente para presentar al directorio, el cual será responsable de adoptar las medidas necesarias.

MATERIALES DE REFERENCIA

Bibliografía

- ALEXANDER, Alberto. (2007), “Diseño de un Sistema de Gestión seguridad de Información”, Primera Edición, Editorial Alfaomega, Bogotá – Colombia, 44-176 pp.

- REYES H., Patricio. (2012), “Administración de Riesgos Medición, Seguimiento, Análisis y Control”, Primera Edición, Editorial Jurídica del Ecuador, Quito – Ecuador, 25 pp.

- SUPERINTENDENCIA DE BANCOS Y SEGUROS (2012), “Capítulo V “De la gestión de riesgo operativo”, del Título X “De la gestión y administración de riesgos”, “Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero.

- ISO/IEC 27001: 2005, Organización Internacional de Estandarización / Comisión Electrotécnica Internacional (2007) “Sistema de Gestión de Seguridad de la Información”.

- ISO/IEC 17799: 2005, Organización Internacional de Estandarización / Comisión Electrotécnica Internacional (2007) “Código de Práctica de Seguridad en la Gestión de la Información”.

- BORTNIK, Sebastián (2010). “Qué es la fuga de información”. (En línea) Disponible en: http://blogs.eset-la.com/laboratorio/2010/04/13/que-es-la-fuga-de-informacion/ (25-02-2012).

- BORTNIK, Sebastián (2011). “La fuga de información preocupa a usuarios, según estudio”. (En línea) Disponible en: http://www.doctortecno.com/article/la-fuga-de-informaci%C3%B3n-preocupa-usuarios-seg%C3%BAn-estudio (25-02-2012).

- CAMELO, Leonardo (2010). “Seguridad de la Información y Seguridad Informática”. (En línea) Disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html (28-02-2012).

- CANO, Jeimy (2008). “Entendiendo la Seguridad de la Información”. (En línea) Disponible en: http://www.acis.org.co/fileadmin/Revista_105/editorial.pdf (20-01-2012).

- GALLARDO, Sara (2009). “Fuga de Información ¿amenaza real?”. (En línea) Disponible en: http://www.acis.org.co/fileadmin/Revista_119/Caraysello.pdf (20-02-2012).

- PACHECO, Federico (2011). “Fuga de Información: ¿una amenaza pasajera?”. (En línea) Disponible en: http://www.eset-la.com/pdf/prensa/informe/fuga_de_informacion.pdf (20-01-2012).

- SUPERINTENDENCIA DE BANCOS Y SEGUROS (2012), “Capítulo V “De la gestión de riesgo operativo”, del Título X “De la gestión y administración de riesgos”, (En línea) Disponible en**:** http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf (18-05-2012).

- WIKIPEDIA, Enciclopedia Libre. (2012) “Investigación Cuantitativa”, (En línea) Disponible en: http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cuantitativa (18-05-2012).

- ESET, Compañía de Soluciones de Seguridad. (2012) “Fuga de Información de Tarjetas de Crédito”, (En línea) Disponible en: http://blogs.eset-la.com/laboratorio/2012/03/30/alerta-fuga-informacion-tarjetas-credito/ (20-04-2012).

- WIKIPEDIA, Enciclopedia Libre. (2009) “Investigación Cuantitativa”, (En línea) Disponible en: http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cuantitativa (20-06-2009).

- EL UNIVERSO, Periódico. (2012) “Advertencia de despidos por ‘fuga’ de información”, (En línea) Disponible en http://www.eluniverso.com/2012/02/08/1/1356/advertencia-despidos-fuga-informacion.html (18-05-2012).

- FABARA, Manolo (2007), “Metodología para la implementación de sistemas seguros de gestión de la información para pequeñas y micro empresas e industrias.”, (En línea) Disponible en: http://repo.uta.edu.ec/handle/123456789/252 (20-05-2012).

- ROJAS, José L. y Vela, Juan J., (1998), “Planificación estratégica y plan de seguridad informática de FABRIL FAME S.A.”, (En línea) Disponible en: http://repositorio.espe.edu.ec/handle/21000/5167 (20-05-2012).

- HARO, Carlos. (2011), “Estudio, diseño y desarrollo de servidores de mensajería instantánea con bases de datos, para la optimización de

recursos en la industria", (En línea) Disponible en: http://repositorio.utn.edu.ec/handle/123456789/604 (20-05-2012).

- VELAZQUEZ, Andrés. (2012), "Delitos informáticos causan pérdidas millonarias en bancos y empresas", (En línea) Disponible en: http://www.enfoqueseguro.com/delitos-informaticos-causan-perdidas-millonarias-en-bancos-y-empresas-2/2012/04/16/estudios del hoy (22-05-2012).

- IT-INSECURITY, Compañía de soluciones de seguridad de la información. (2009) "La cultura de seguridad de la información", (En línea) Disponible en: http://insecurityit.blogspot.com/2009/08/cultura-de-seguridad-de-la-informacion.html (24-05-2012).

- WIKIPEDIA, Enciclopedia Libre. (2011) "Seguridad de la Información", (En línea) Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n (18-05-2012).

- SHOSTACK y Stewart. (2008), "Entendiendo la inseguridad de la información" , (En línea) Disponible en:

  http://www.acis.org.co/fileadmin/Revista_105/editorial.pdf (20-05-2012)

- CAMELO, Leonardo. (2010), "Seguridad de la información y seguridad informática", (En línea) Disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html (21-05-2012).

- SOLA S., Jordi. (2011), "Seguridad de la información y seguridad informática", (En línea) Disponible en:

http://www.revistasic.com/revista61/pdf_61/SIC%2061_quepreocupa.PDF (22-05-2012).

- MORALES., Frank. (2010), “Tipos de Investigación”, (En línea) Disponible en:

  http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa (23-05-2012).

- HERRERA E., y otros. (2012), “La Operacionalización de Hipótesis”, (En línea) Disponible en: http://vhabril.wikispaces.com/file/view/6UTA.+Hipótesis+y+Variables+-+Abril+PhD.pdf (23-05-2012).

- VICH, Raza y ARY. (1992), “El cuestionario”, (En línea) Disponible en:
  http://books.google.com.ec/books?id=B2L6wakmpIwC&pg=PA91&lpg=PA91&dq#v=onepage&q&f=false (23-05-2012).

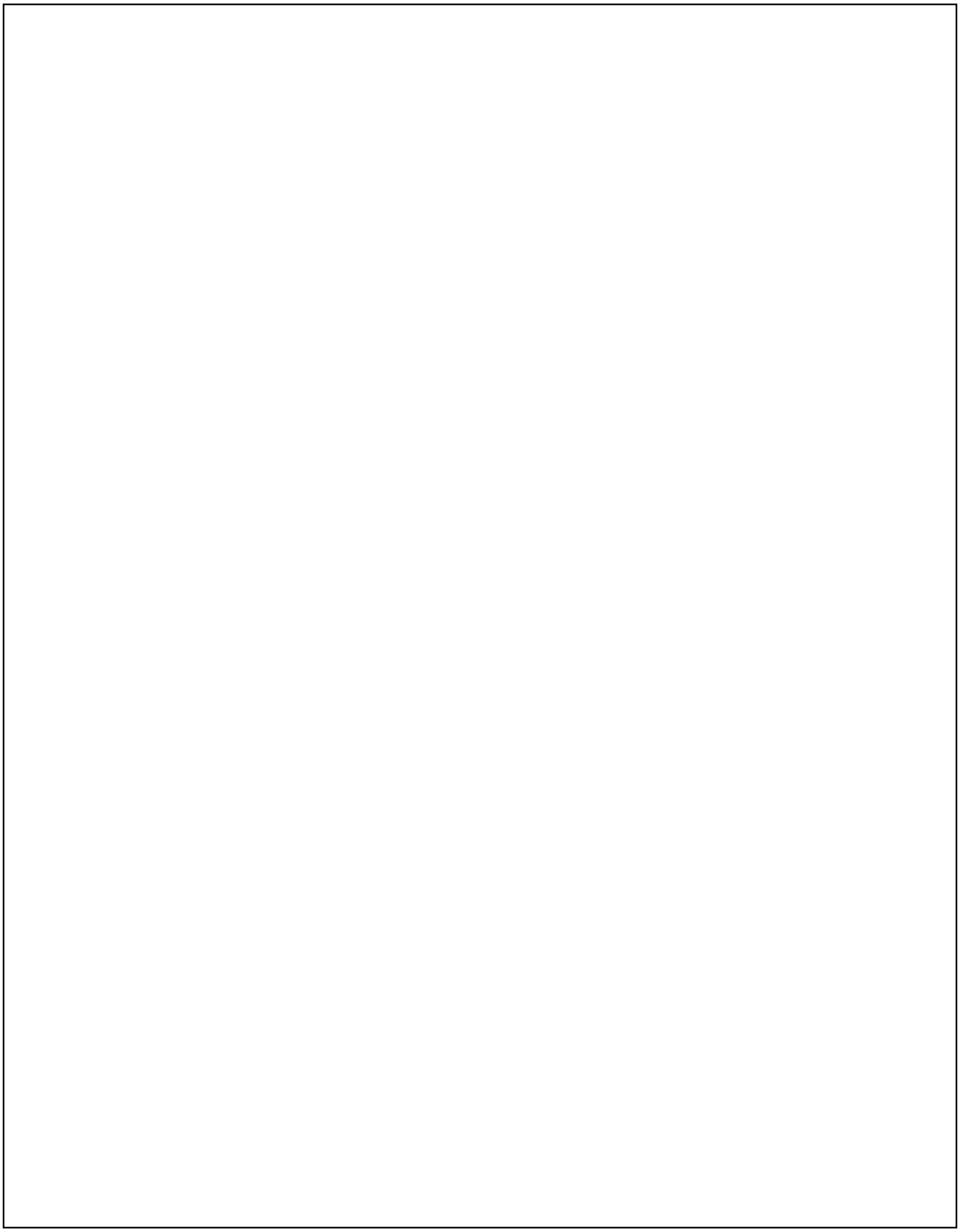
- RUIZ, Ramón. (2008), “Definición de Método Deductivo e Inductivo”, (En línea) Disponible en: http://definicion.de/metodo-deductivo/ (23-05-2012).

LOPEZ C., José L. (2008), “Métodos de Investigación”, (En línea) Disponible en: http://www.monografias.com/trabajos11/metods/metods.shtml (23-05-2012).

ANEXOS

A1

REGISTRO ÚNICO DE CONTIBUYENTE - RUC



Fuente: Investigación de Campo

Elaborado por: LÓPEZ, Mariela (2012)

A2

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD CONTABILIDAD Y AUDITORIA

MAESTRÍA EN GESTIÓN FINANCIERA

Objetivo.- Evaluar el grado de cultura en seguridad de la información del personal de Unifinsa.

Indicaciones

1.- Comedidamente solicito a usted se sirva contestar el cuestionario que se presenta a continuación.
2.- En caso de duda, favor consultar al encuestador.
3.- Por favor marque con una x su respuesta.
4.- Agradezco su tiempo y colaboración.

ENCUESTA

Cuestionario 1

1. ¿Usted ha participado en algún programa de capacitación referente a cultura en seguridad de la información en Unifinsa en el año 2011?

   ( ) Si
   ( ) No

2. ¿Ha dejado desprotegido el equipo en horas laborables?

   ( ) Si
   ( ) No

   En caso de ser afirmativa o negativa su respuesta mencione ¿Por qué?

   _____
   _____

3. ¿Qué riesgo corre al dejar desprotegido su equipo de cómputo cuando se ausenta de su lugar de trabajo?

( ) Riesgo Alto
( ) Riesgo Medio
( ) Riesgo Bajo
( ) Ningún Riesgo

¿Por qué?

_____
_____

4. ¿Puede Usted identificar que una información es de carácter confidencial?
   ( ) Si
   ( ) No

5. ¿Puede Usted identificar que una información es de carácter pública?

( ) Si
( ) No

6. ¿Ha asistido a charlas en Unifinsa en el año 2011, acerca de pérdida de confidencialidad?

( ) Si
( ) No

¿Cuántas veces?

_____

7. ¿Necesita Usted recibir capacitación en temas relacionados con pérdidas de confidencialidad?

( ) Si
( ) No

8. ¿Ha asistido a charlas en Unifinsa en el año 2011, respecto a fuga de información?

( ) Si
( ) No

¿Cuántas veces?

_____

9. ¿Necesita Usted recibir capacitación en temas relacionados con Fuga de Información?

   ( ) Si
   ( ) No

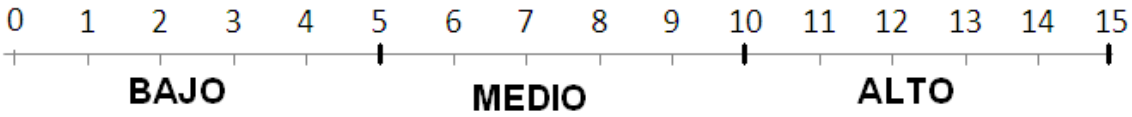
10. ¿Conoce Usted las políticas de seguridad de la información referentes a la protección de la información confidencial?

    ( ) Si
    ( ) No

11. ¿Conoce usted de algún procedimiento para desechar reportes impresos que contienen información confidencial?

    ( ) Si
    ( ) No

12. ¿Autocalifique su grado de cultura en temas de seguridad de la información? Encerrar el número en un círculo.



    ¿Por qué se autocalifica de esa manera?

    _____
    _____
    _____

13. Teniendo en cuenta que solo el 20% de los colaboradores han recibido la capacitación en temas relacionados con seguridad de la información. ¿Qué falencias presenta Usted en el proceso?

( ) a) Desconocimiento de las políticas de seguridad de la información
( ) b) Desinterés en temas relacionados con seguridad de la información
( ) c) Incumplimiento de políticas de seguridad de la información
( ) Todas las anteriores
( ) a) y b)
( ) b) y c)
( ) a) y c)

14. Ordene cada uno de los medios de información, sujetos a pérdida de confidencialidad que a su criterio genera mayor riesgo en la organización. Considerando que 1 es riesgo muy alto y 6 es riesgo extremadamente bajo.

( ) Documentos Fotocopiados
( ) Documentos Impresos
( ) Discos Compartidos
( ) Salida del Personal
( ) Correo Electrónico
( ) Flash Memory o discos Externos

¿Por qué considera que el número (1) es el medio de pérdida de confidencialidad que genera mayor riesgo?

_____
_____
_____

15. ¿Indique si la implementación de un plan de tratamiento de riesgo contribuirá al control de la fuga de información en Unifinsa?

( ) Si
( ) No

16. ¿El desconocimiento de la cultura en seguridad de la información es lo que produce pérdida de confidencialidad en Unifinsa?

( ) Si
( ) No

¡Muchas Gracias por su ayuda!

A3

Robo de información a lo largo del 2011 (2da parte)

noviembre 15. 2011 4:43 pm

Hace un tiempo atrás, publicamos en el blog una recopilación de casos de fuga de información ocurridos en varias empresas de renombre a lo largo del 2011. Esta información previamente publicada, abarco el período comprendido entre enero y mayo. A continuación analizaremos esta amenaza a partir de esa fecha hasta hoy:

Luego de la intrusión en los sistemas de PlayStation Network, el grupo Lulzsec atacó a la productora de televisión y cine Sony Pictures. Entre la información divulgada, se obtuvo la base de **datos de 1.000.000 de usuarios de Sony** donde las contraseñas se encontraban **sin ningún tipo de cifrado**.

La empresa productora de computadoras Acer sufrió un acceso a través de su servicio de FTP. Los delincuentes digitales se hicieron con los datos de **40.000 clientes de la empresa y diversos códigos fuentes que se encontraban en el servidor**.

InFraGard una filial del FBI, fue víctima del robo de 120 cuentas de sus miembros. Con el acceso a estas cuentas, se podía **acceder a información sensible de la organización**.

La comunidad de lectura Writespace sufrió la **publicación de 62.000 credenciales (contraseñas y correos electrónicos)**. Dicha publicación fue realizada por el grupo Lulzec.

El banco Citigroup durante este año ha sufrido **dos grandes casos de fuga de información**. En el primero, las víctimas implicadas fueron **200 mil clientes en Estados Unidos** donde obtuvieron los **nombres, números de cuenta y números de las tarjetas de los afectados**. En el segundo robo de información que sufrió la entidad financiera, fueron **afectados 92.000 clientes de origen japonés**, y nuevamente los datos filtrados fueron los **nombres, usuarios y números de tarjetas**.

La base de datos de **Orange Francia fue filtrada a través de la red social Twitter** con el código fuente del sitio web. El ataque se atribuye al grupo Anonymous.

El sitio de transacciones de propiedades BlueHomes sufrió un ataque en donde se filtró información de sus clientes. El autor del hecho, publicó la información de **500.000 usuarios en una aplicación web para subir texto**.

Steam, la plataforma de videojuegos de Valve, sufrió un ataque a sus bases de datos. En el comunicado dado por la empresa, se informó que los criminales informáticos tuvieron **acceso a nombres de usuarios, contraseñas y números de las tarjetas de crédito de los afectados**. Afortunadamente, estos últimos se encontraban cifrados dificultando la tarea del atacante.

Vemos que el panorama no cambio mucho desde la última publicación, cada vez son más empresas las que sufren problemas de fuga de información. El impacto producido depende de l**a sensibilidad de los datos filtrados**. Es por eso, que es importante **implementar y controlar diariamente las medidas de seguridad implementadas en los sistemas** y así poder evitar este problema conocido hace bastante tiempo.

Claudio Cortés Cid
Especialista de Awareness & Research