UNIVERSIDAD APEC

ESCUELA DE GRADUADOS

Monográfico para optar por el título de:

MAESTRÍA EN GERENCIA Y PRODUCTIVIDAD

"Impacto del Grado de Conocimiento de los Empleados Sobre las Políticas de Seguridad de Sistemas de Información en la Confidencialidad, Disponibilidad e Integridad de la Información Importante de la Empresa." Caso: EXTRA-SEGUROS, *SA*. 2009.

Sustentante:

Cristina Jiménez Vásquez 2007-2313

Asesor:

Prof. Edmundo Morel

Santo Domingo, D. N.

Agosto 2009

Dedico este trabajo a Dios y todas las personas que me han apoyado en el logro de esta nueva meta en mi vida.

AGRADECIMIENTOS

Un especial agradecimiento **a mi propio ser**, **a mi hijo Emmanuel y a mi esposo Lisandro,** por todo el apoyo que me brindaron cediéndome parte importante de su tiempo.

A mi amiga Hellen por ser mi principal motivadora, quien con sus frases hizo que sacara de mí lo mejor.

A Tania por su amistad y comprensión ayudándome siempre que lo necesitaba.

A Pedro Feliz por haberme ayudado a elegir este tema tan interesante y por toda su orientación.

Resumen

La información generada por las empresas constituye un recurso vital para la toma de decisiones y orientación de las estrategias a seguir en el logro de su visión. Esto hace necesario que se implementen medidas o políticas de seguridad que garanticen la disponibilidad, integridad y confiabilidad de la misma al momento de ser utilizada.

Las empresas crean en su estructura departamentos de seguridad de la información que se encargan de crear políticas o medidas que aseguran la calidad de la información, así como de todos los aspectos necesarios para la implementación de dichas políticas.

En esta investigación se plantea que el departamento de seguridad de la información debe comunicar a los empleados las políticas necesarias en la empresa, para que su implementación sea más efectiva y a la vez sean asimiladas como parte de sus funciones, garantizando así que la información sea menos vulnerable.

La asegurabilidad de la información depende de múltiples factores y aunque el encargado de administrarla implemente todas las medidas posibles, nuevas formas y vulnerabilidades se van creando, que no permitirán que la información sea segura en un 100%, sin embargo su protección es indispensable.

De los empleados depende el cumplimiento de una parte importante de las medidas de seguridad de la información de las empresas, motivo por el cual hacerlos conscientes del beneficio o la razón de ser de éstas, hace que su compromiso de cumplirlas sea mayor, como se muestra en los resultados de esta investigación.

El estudio de este interesante tema fue llevado a cabo en la empresa de seguros Extra-Seguros SA., prestigiosa empresa de la República Dominicana, por medio a encuesta aplicada a los empleados de todos los niveles y una entrevista al administrador de seguridad de la información.

Palabras claves:

Seguridad de la Información – Comunicación Empleados – Implementación Políticas de Seguridad.

INDICE

CONTENIDO

CUADROS

GRAFICOS

APENDICES

INTRODUCCION

I. INTRODUCCION

1.1 Definición del problema.

Uno de los mayores desafíos de las empresas actuales, independientemente de su tamaño o sector de actividad, es garantizar que la información, su principal activo, se encuentre protegida y a salvo de personas malintencionadas o no autorizadas.

En el mundo de los negocios cada vez más se requiere asegurar la confiabilidad, confidencialidad y la integridad de la información, ya sea para garantizarles confianza a los clientes, como para garantizar las operaciones estratégicas de la empresa.

Aunque muchos opinan que hablar de garantizar la seguridad de los sistemas de información en un 100% es un tema utópico, también es muy cierto que no tomar medidas en este sentido es el peor riesgo que puede tener una empresa que desea mantenerse competitiva en su industria hoy día.

Las empresas, conociendo la importancia y el valor de la información que manejan en sus sistemas, utilizan herramientas que contribuyen a minimizar el grado de vulnerabilidad ante daños intencionales o no a su información, debiendo también mantenerse monitoreando sus sistemas y conexiones para

identificar nuevas causas o fuentes de vulnerabilidad y buscar nuevas técnicas para la protección de este importante activo.

La tendencia es que la información sea cada vez más expuesta y por ende más vulnerable, ya que cada día se integran nuevos saboteadores de la información a través del internet y además la falta de ética y responsabilidad de quienes la manejan o administran. Tanto el control del internet como la ética de los empleados de las empresas son elementos indispensables para el manejo seguro de la información.

Los empleados de las empresas constituyen un gran riesgo para la integridad y confidencialidad de la información, ya que la mayoría de las veces no son conscientes de la importancia de conocer y aplicar las políticas de seguridad establecidas por la empresa para garantizar la seguridad de la información que manejan. Esto es debido a que los ejecutivos no han tomado las medidas adecuadas o pertinentes para que los empleados sean parte interesada de cuidar la información y no un ente desintegrador de la misma.

Esta situación hace necesaria la implementación de métodos para lograr el compromiso de los empleados, sobre la importancia del conocimiento y el cumplimiento de las políticas de seguridad de la información y el impacto que puede traer consigo el no cumplimiento de las mismas, para ellos y para la empresa. Extra-Seguros no es la excepción de esta problemática; pues es una empresa que maneja un gran volumen de información y a pesar de poseer un

departamento para el manejo de la seguridad de los sistemas y de la información no ha logrado que sus empleados interioricen la responsabilidad para cumplirla.

De acuerdo al problema definido anteriormente se ha formulado la siguiente pregunta como problema de investigación:

¿Cómo ha impactado el grado de conocimiento de los empleados de Extra-Seguros de las políticas de seguridad de sistemas de información, en la confidencialidad e integridad de la información importante de la empresa?

Dicha pregunta general podría desglosarse en las siguientes preguntas específicas:

1. ¿Por qué es tan importante la protección de la información crítica en la empresa en el día de hoy?
2. ¿Cómo influye la comunicación en la implementación de las medidas de seguridad de información establecidas en la empresa?
3. ¿Cómo ha sido el nivel de cumplimiento de las políticas de seguridad en Extra-Seguros?
4. ¿Qué impacto ético tiene la violación de las políticas de seguridad por parte de los empleados de una empresa?
5. ¿Cómo impactaría el conocimiento de los empleados de la empresa de las políticas de seguridad de la información en la confiabilidad e integridad de la información crítica de Extra-Seguros?

1.2 Objetivos de la investigación.

Objetivo General:

Determinar el impacto del grado de conocimiento de los empleados de Extra-Seguros sobre las políticas de seguridad de sistemas de información, en la confidencialidad e integridad de la información crítica de la empresa.

Objetivos específicos:

- Conocer la importancia de la protección de la información de las empresas en el día de hoy.
- Conocer la influencia de la comunicación en la implementación de las políticas de seguridad de una empresa.
- Determinar el nivel de cumplimiento de las políticas de seguridad en Extra-Seguros en el 2009.
- Conocer el impacto ético que tiene la violación de las políticas de seguridad por parte de los empleados de una empresa.
- Determinar el impacto en la confiabilidad e integridad de la información de Extra-Seguros al concientizar a los empleados en las políticas de seguridad de la empresa.

1.3 Justificación del estudio.

Con este estudio se pretende dar a conocer a los ejecutivos de Extra-Seguros la necesidad de implementar mecanismos de educación y concientización a los

empleados, sobre el conocimiento y aplicación de las políticas de seguridad establecidas por la empresa, destacando la importancia de una información íntegra y confiable.

Evans y Linsdsay (2008) definen la información como: “La información son los datos en el contexto de un negocio u organización que permiten a los directivos tomar decisiones basadas en hechos y no en opiniones. Es utilizada para guiar a la organización en una dirección en particular, es decir, para dirigir las estrategias y el cambio organizacional”.

Bajo esta definición se puede decir que la información es uno de los activos más importantes que tienen las empresas. Prácticamente todos los aspectos de un negocio dependen de la aceptación de los datos procesados y la provisión oportuna de la información.

Normalmente las informaciones de las empresas revisten un alto grado de confidencialidad, lo cual requiere establecer controles en su resguardo y divulgación. Este proceso sólo se consigue si los sistemas de información están protegidos contra amenazas.

Por tales razones se hace imprescindible la protección de la información, a manera de asegurar su confidencialidad, integridad y disponibilidad; siendo estas tres características los principios básicos de la seguridad de la información.

Normalmente las medidas para protección de la información sugeridas por la administración de la seguridad de la información en las empresas son un tanto incómodas y molestas para los empleados, como son, muchas claves para recordar, restricciones de uso del internet, restricciones de uso de dispositivos de entrada y salida, entre otros. Por esto debe evitarse por todos los medios la imposición forzada de dichas medidas, ya que sólo con factores positivos se podrán obtener los mejores resultados.

Las personas son el elemento más importante de un programa de Seguridad de la Información, pues la difusión de la información está bajo su control y como existen actualmente tantas formas para evadir controles, es necesario que se concienticen para que dicho programa se cumpla satisfactoriamente.

El conocimiento y entrenamiento sobre la seguridad, por ende, es esencial. Los empleados necesitan ser informados y advertidos sobre las amenazas, represalias y responsabilidades del manejo de la información; pues cuando se establece una correcta comunicación, se facilita el trabajo en cuanto al logro del cambio necesario, y la participación masiva e inteligente en aras de lograr un compromiso consciente y entusiasta de todos los miembros de la entidad.

Los resultados de esta investigación serán de mucha utilidad para Extra-Seguros SA en su objetivo de seguir avanzando en su posicionamiento en el mercado asegurador Dominicano. Cuanto más relevante y útil sea la información

sobre el negocio, clientes, socios y operaciones, mejores serán las decisiones que podrá tomar la organización para lograr mejores ventajas competitivas.

MARCO TEORICO

II. MARCO TEÓRICO

2.1 Información y Sistemas de Información.

Para entender todos los aspectos de funcionamientos de la seguridad informática, se debe analizar primero qué es la información y cómo se almacena, para así delimitar los riesgos; luego se debe ser conscientes de que dicha información se encuentra almacenada y procesada en computadoras, además se debe reconocer que ésta debe ser confidencial y por eso, se crean riesgos, pues puede ser robada, mal utilizada o divulgada por personal no autorizado.

La información es clave para el crecimiento y éxito de una empresa, un buen sistema de gestión de la información demuestra a los clientes de una empresa que su información cuenta con la protección adecuada tanto en papel, electrónica y en la mente de los empleados.

Como explica Evans y Linsdsay (2008), “la información son los datos en el contexto un negocio u organización que se deriva del análisis de datos suministrados. Las organizaciones necesitan la información para guiar la empresa en el logro de la estrategia trazada. La información es la materia prima que alimenta la toma de decisiones en todos los niveles de la organización. Y normalmente se encuentra almacenada en la base de datos de los sistemas de información de las empresas”.

Por medio al procesamiento de la información, las compañías crean valor, ya que ésta ayuda a alcanzar los objetivos de la compañía.

Un sistema de información integra todos los elementos que forman parte de la administración, el procesamiento, la distribución y el transporte de la información dentro de una compañía. En términos prácticos, el alcance del término "sistema de información" puede variar notablemente entre una empresa y otra y, según el caso, puede abarcar elementos como bases de datos, software de gestión, servidores de datos, sistemas de almacenamiento, servidor de aplicaciones, dispositivos de seguridad, entre otros.

La información de las empresas, por su vital importancia, hace que muchos técnicos buenos trabajen para fortalecer la seguridad de la información en los sistemas de información. Estos técnicos desarrollan seguridad lógica que consisten en barreras y procedimientos que resguarden el acceso a los datos, permitiendo que sólo sean vistos por el personal autorizado. Esto es, se hacen pensando en los siguientes factores: se deben actualizar las contraseñas constantemente, los técnicos se aseguran de que los operadores puedan trabajar con cierta información pero que no puedan modificarla, se restringe el acceso a un grupo de programas y archivos, etc.

La manipulación de datos se puede dar tanto dentro de la empresa, como de manera virtual. La seguridad en sistemas de información además contempla una batalla, hoy día, contra los virus informáticos; que no son más que

programas elaborados intencionalmente que se introducen y transmiten entre los discos o redes de comunicación de los computadores y servidores causando diversos tipos de daños en los equipos. Unas veces, estos daños pueden ser solo físicos, es decir, se daña un componente del equipo, mientras que en muchas ocasiones resulta ser virtual, se daña una pieza de la máquina pudiendo llevar a la pérdida de información que está almacenada.

2.2 Seguridad de la información o seguridad informática.

Oz (2008) señala que “La preocupación principal de cualquier organización debe ser sus datos, porque suele ser un recurso único. Los datos recopilados con el tiempo casi nunca se pueden recuperar del mismo modo, e incluso cuando esto es posible, el proceso es demasiado costoso y tarda mucho tiempo para recuperar las pérdidas del negocio. Todos los datos y aplicaciones son susceptibles de interrupción, daño y robo”. Y señala también que “en ocasiones la negligencia de las corporaciones y el uso descuidado de la tecnología, sobre todo en las conexiones públicas de internet, crean “huecos” o vulnerabilidades en la seguridad”.

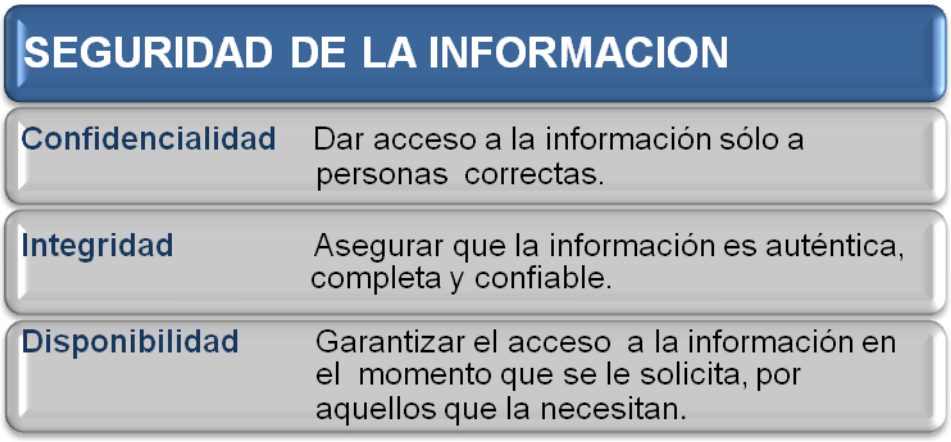
La Seguridad de la información es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recurso humano integrado para proveer toda la protección debida y requerida a la información y a los recursos informáticos de una empresa.

Los sistemas de información son a veces vulnerables y se producen alteraciones o fallas en los datos que poseen las empresas, debido a que existen personas que desean corromperlos o introducirse en ellos sin autorización. Como este severo problema se hacía cada vez más frecuente en las empresas, se introdujo el concepto de seguridad en sistema de información, también conocido como seguridad informática.

La evolución tecnológica genera cada vez, más y más facilidades para almacenar, analizar o procesar datos, produciendo a su vez riesgos que en ocasiones pueden ser críticos para las empresas. Dichos riesgos han hecho que técnicos experimentados dediquen su tiempo a innovar en los aspectos de seguridad de sistemas de la información para que estos datos sean lo menos vulnerable posible.

Un sistema seguro debe proteger la información vista en tres dimensiones, la primera es la disponibilidad, es decir, la información debe estar disponible cuando se le necesita; la segunda es la integridad, dicha información no puede ser modificada por personal no autorizado; y la tercera es la confidencialidad, la información debe ser accesada sólo por quienes están autorizados. Como se puede ver en el siguiente cuadro.

Cuadro 1. Dimensiones de la Seguridad de la información



Fuente: Microsoft 2009. http://www.microsoft.com/conosur/proseguridad/informacion.aspx

2.3 Políticas de Seguridad informática.

Las empresas buscan medidas para proteger su información y dentro de éstas están la creación de un departamento que diseñe políticas y regule su cumplimiento con eficiencia y criterio. Este departamento se encarga de crear las políticas de seguridad que protejan la información de tanta vulnerabilidad.

Las Políticas de Seguridad Informática (PSI), nacen como una herramienta organizacional para concientizar a los miembros de las empresas, sobre la importancia y sensibilidad de la información y los servicios críticos.

Huerta (2000), señala que "Una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos

generales qué está y qué no está permitido en el área de seguridad durante la operación general del sistema."

SPAFFORD (2000) en su Manual de seguridad en redes dice que la política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "...una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas" y debe:

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Oz (2008) afirma que “las medidas de seguridad hacen lentas las comunicaciones de datos y requieren disciplina del usuario, la cual no es fácil de mantener. Los empleados tienden a olvidar sus contraseñas, sobre todo si

deben cambiarlas cada 30 o 90 días". Además argumenta que "a los empleados les molesta mucho tener que recordar una contraseña diferente para cada sistema que usan. Los especialistas de la administración de la seguridad deben explicar con claridad a los administradores las implicaciones de aplicar medidas de seguridad y deben comunicar a los empleados el impacto que tendrá una nueva medida de seguridad en su actividad diaria y si afectará de manera adversa su trabajo y se deben convencer a los empleados de que esa incomodidad es el precio de proteger los datos".

En estudio realizado por Cisco Systems Inc. (2008), para detectar los errores comunes que cometen los empleados, determinó que para reducir la fuga de datos, las empresas deben integrar la seguridad en su cultura empresarial y evaluar constantemente los riesgos de cada interacción con redes, dispositivos, aplicaciones, datos y, por supuesto, otros usuarios. De acuerdo a dicho estudio las empresas deben comenzar por evaluar la conducta de los empleados y los riesgos asociados basándose en factores tales como el país y el panorama de amenazas. Luego de acuerdo con dicha evaluación pueden diseñarse planes de educación sobre amenazas, capacitación en seguridad y procesos comerciales. Ése es el momento de realizar inversiones pertinentes en tecnología de seguridad.

Cisco Systems también dice que el personal suele ver a la tecnología de información y la política de seguridad como un estorbo para su productividad.

Izquierdo (2009), director de INTECO (Instituto Nacional de Tecnologías de la Comunicación, España) destaca que la necesidad de promover una cultura formativa en seguridad y concienciar a los usuarios ha sido uno de los puntos destacados, porque considera que "el eslabón más débil en la cadena de seguridad corporativa siempre es el empleado mal informado". Según Izquierdo, "el 62% de las pérdidas de información en las empresas se deben a errores de los empleados y no a ataques".

Por otra parte, para denotar la importancia de que los empleados se entrenen en cuanto a las políticas de seguridad para el mejor manejo de las informaciones críticas de la empresa, se han hecho algunas investigaciones como se presenta a continuación.

Tirado (2009) en su trabajo el 'Enemigo Interno' dice que se estima que el 82% de la pérdida de datos sensibles de una compañía la producen los mismos empleados. El 80% de los equipos portátiles que la organización asigna a su personal es compartido con terceros, lo que abre la puerta al ingreso de virus y programas peligrosos para los sistemas empresariales.

Al hablar de seguridad, Tirado (2008) argumenta que " la gran mayoría de los especialistas y de los administradores de tecnología de información están de acuerdo en que el eslabón más débil de la cadena es el usuario. Desde un gesto inocente como prestarle a un compañero de trabajo el nombre de usuario y clave de acceso para ingresar a la red, hasta el robo de información confidencial de

los clientes, la realidad indica que son los causantes de más del 60% de las fallas en los sistemas de las empresas". Además dice que es importante destacar que muchas de las brechas de seguridad se dan por simple desconocimiento. No saber que existen ciertos mecanismos de protección dentro de la empresa, o no tener actualizado el antivirus, son algunos factores que pueden ser de mucha importancia.

Algunas medidas o políticas de seguridad de la información básicas, que involucran a los empleados de las empresas son las siguientes:

Cuadro 2. Ejemplos de políticas básicas de seguridad de la información

Políticas de Seguridad Empleados	
1.	Usa tu puesto de trabajo con profesionalidad.
2.	Mantén orden y limpieza. Donde hay caos, hay riesgo.
3.	Instala y utiliza únicamente programas y dispositivos proporcionados por empresa.
4.	La información confidencial no está sólo en el ordenador. Ten cuidado con el papel u otros soportes (disquetes, CD-ROM, memorias portátiles, etc.).
5.	Antes de proporcionar cualquier información, comprueba a quién y cómo la debes comunicar (Teléfono, e-mail, fax, etc.).
6.	No comuniques tus contraseñas. Protégelas y cámbialas a menudo.
7.	No pierdas información, haz copias en las carpetas de red.
8.	Evita las webs y correos sospechosos.
9.	Protege tu computador Bloquea el equipo cuando no lo uses …
10.	Si tienes dudas consulta a tu supervisor, etc.

Fuente: Elaboración Propia. Políticas de seguridad Extra-seguros SA.2009

2.4 Manual de Políticas de seguridad de la información.

La formalización o planificación de las políticas de seguridad de una empresa debe hacerse mediante un documento formal o plan, que contenga toda la estrategia de seguridad para preservar la integridad de la información.

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles debiendo abarcar seguridad física, lógica, humana, y la interacción que existe entre todos estos factores.

El manual de políticas de seguridad de la información no debe ser una descripción técnica, ni una expresión legal de mecanismos de seguridad, es más bien una descripción de lo que se desea proteger y la razón de ser de ello.

Según BENSON (2000), en cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y otra Reactiva. La Estrategia Proactiva (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque, ayudará a desarrollar esta estrategia.

La Estrategia Reactiva (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a

repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Por otro lado BENSON (2000) expresa que se pueden tomar dos posturas básicas , que puede adoptarse ante los recursos compartidos en la empresa, la primera dice que lo que no se permite expresamente está prohibido, significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida. Y la segunda dice que lo que no se prohíbe expresamente está permitido, significando que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.

2.5 Factores de riesgo.

En la investigación realizada por Tirado (2009), en su trabajo el 'Enemigo Interno' describe algunas conclusiones y opiniones de otros estudios realizados sobre la seguridad de la información en las empresas y la relación de ésta con los empleados y dice como sigue:

> De acuerdo con el “Estudio global sobre estado de la seguridad de la información” presentado por Deloitte a principios de este año (2009), la región de Latinoamérica reportó que poco más de la mitad de las empresas consultadas han realizado algún tipo de concientización o campañas de educación de usuarios sobre seguridad informática en los últimos 12 meses. En ese mismo período, más del 65 por ciento de las firmas encuestadas en esa región han sufrido algún tipo de brecha de seguridad.”
>
> De acuerdo con André Monteiro, director de Seguridad de Computer Associates (CA) para América Latina, “la falta de una cultura informática puede ser un factor de riesgo importante, ya que muchas personas deshabilitan los programas de seguridad instalados en las computadoras, tales como el antivirus, el anti-spyware o firewall, pero mucho de lo que ocurre es por el desconocimiento de los daños que pueden ocasionar”.

Tirado (2009) también habla sobre la desinformación, y dice que existen dos caras de una misma moneda. ” Por una parte, en un entorno empresarial no todos los usuarios de los equipos de cómputo tienen que ser especialistas técnicos o conocedores de las últimas tendencias y amenazas de seguridad. Desde el punto de vista práctico, tener a todo el personal capacitado en materia de tecnología de la información y los consecuentes riesgos es virtualmente imposible.

Según esta investigación la pérdida de información, sea por las razones que sea, es una de las mayores preocupaciones de las altas gerencias hoy en día. Más aun si se toma en cuenta que, según Juan Pablo Castro, consultor de Tecnología de Trend Micro México, “alrededor del 82 por ciento de los casos en los que se pierde información sensible o confidencial de una empresa se produce en manos del personal interno”.

Oscar Campos Solano, consultor sénior de Seguridad para la firma PricewaterhouseCoopers, comentó en el estudio de Tirado (2009), que estas grietas en los sistemas de seguridad, pueden suceder por varios factores. En primer lugar están las contraseñas débiles o configuradas por defecto, que son de fácil deducción. “En muchos casos, debido a la urgencia de habilitar un servicio para atender al negocio, se instalan aplicaciones en forma apresurada, lo que conlleva a que el administrador no pueda implementar medidas de seguridad para prevenir accesos no deseados”,

Por otra parte, la investigación señala que para André Monteiro, el 80 por ciento de los equipos portátiles asignados por la organización a sus empleados son compartidos por integrantes del hogar u otras personas y, a pesar de que en sí mismo no es un riesgo, el peligro se presenta cuando se instalan programas ajenos a la organización que pueden ser de dudosa procedencia. “Otra importante fuente de riesgo es navegar por sitios que pueden hacer que tanto la

integridad de la computadora como de la empresa se vean comprometidas", agregó Monteiro.

Otras opiniones presentadas por Tirado en su trabajo el 'Enemigo Interno' son las de Flavio de Cristófaro, Cristian Borghello, el estudio presentado por Trend Micro y Casas de Deloitte, y son las siguientes:

Para Flavio de Cristófaro, gerente de Seguridad y Servicios de Privacidad de Deloitte, el impacto que puede llegar a tener que un usuario que esté usando Internet de forma indebida tiene un costo altísimo para una compañía. Para el especialista, también hay que considerar otros aspectos que no son tan cuantificables, como es el desgaste de la imagen de la empresa frente al cliente.

Sobre este aspecto, Cristian Borghello, gerente Técnico y Educativo de ESET para Latinoamérica, agregó: "la descarga de archivos es crítica, ya que existen malware que se propagan por correo, mensajería instantánea y sitios web automáticamente sin que el usuario lo note". De acuerdo con el especialista, hoy casi cualquier lugar en la red es una posible fuente de infección.

Para Borghello, de ESET, "los dispositivos de almacenamiento masivo, memorias y discos portátiles son un gran problema, porque permiten la proliferación de todo tipo de malware". Sobre este aspecto, Cristian Borghello, agregó: "la descarga de archivos es crítica, ya que existen malware que se propagan por correo, mensajería instantánea y sitios web automáticamente sin

que el usuario lo note". De acuerdo con el especialista, hoy casi cualquier lugar en la red es una posible fuente de infección. Los diferentes gadgets que son tan comunes, como pendrives o discos USB, presentan una comodidad a la hora de compartir o transportar información pero, al mismo tiempo, son una fuente de infección y de penetración de los equipos donde se utilizan.

Según un estudio presentado por Trend Micro, entre los principales vectores de fuga están los dispositivos USB y luego el mail corporativo, el correo social, como Yahoo! o Hotmail y, por último, la mensajería instantánea.

Casas, de Deloitte definió que "el éxito de un programa de concientización se da cuando los usuarios comprenden el impacto que tienen sus acciones detrás de eventos como abrir sus correos personales o ejecutar programas ajenos a la empresa".

Por otra parte, fuera del estudio de Tirado, se tiene que en el estudio realizado por Cisco Systems Inc. (2008), se pudieron establecer cuáles son las principales conductas que ponen en riesgo la seguridad de los datos al interior de las compañías. La investigación descubrió que a pesar de las políticas, procedimientos y herramientas de seguridad actualmente en uso, los empleados de todo el mundo exhiben conductas arriesgadas que ponen en peligro los datos personales y empresariales

Y este estudio dio como resultado lo siguiente:

● **Uso de aplicaciones no autorizadas:** el 70% de los profesionales de Tecnología de información cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.

● **Uso indebido de computadoras de la empresa:** el 44% de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.

● **Acceso no autorizado tanto físico como a través de la red:** el 39% de los profesionales de Tecnología de información (TI) afirmó que ha debido abordar el acceso no autorizado por parte de un empleado a zonas de la red o de las instalaciones de la empresa.

● **Seguridad de trabajadores remotos**: el 46% de los empleados admitió haber transferido archivos entre computadoras del trabajo y personales al trabajar desde el hogar.

● **Uso indebido de contraseñas**: el 18% de los empleados comparte contraseñas con sus colegas.

Sin duda que aunque gran parte del peligro proviene desde redes externas (por ejemplo Internet), los continuos esfuerzos del personal de Tecnología de información (TI) por prevenir las fugas de información dentro de las redes de la compañía se ven mermados por este tipo de comportamientos de los usuarios

finales que muchas veces son causadas por ignorancia, descuido o mala intención.

Microsoft (2009) señala que la importancia de contar con políticas de seguridad claras y firmes es innegable. Por lo que es importante tomar conciencia de la cantidad de factores que atentan contra el buen funcionamiento de los sistemas, y la confidencialidad, integridad y disponibilidad de sus datos. También dice que sorprendentemente, en la mayoría de los casos, los factores de riesgo no siempre están relacionados con la tecnología., sino que dependen de medidas internas mayormente. A continuación algunas consecuencias del riesgo de la falta de seguridad:

Gráfico 1. Consecuencias por falta de seguridad de la información

Fuente: Microsoft en http://www.microsoft.com/conosur/proseguridad/informacion

Pallavicini (2009) dice que se debe considerar que estadísticas a nivel mundial y con mayor razón en Latinoamérica, además muestran que el 85% de los fraudes en las empresas son hechos por gente interna o ex empleados de la Compañía

2.6 Comunicación y hábitos de seguridad.

Plamondon (2006) en su artículo: Cómo ayudar a sus empleados a adquirir mejores hábitos de seguridad, detalla lo siguiente:

“Las acciones de los usuarios tienen un impacto enorme en la seguridad de los equipos, de modo que la educación de los empleados, así como la de los miembros del departamento de Tecnología de la información y la dirección, es un requisito fundamental para que reconozcan el carácter prioritario de la seguridad y desarrollen buenos hábitos al respecto.

Plamondon (2006) también dice en su artículo que Según O'Leary, la gente necesita razones, tanto positivas como negativas, para modificar su comportamiento. En el ámbito de la seguridad, esto conlleva la necesidad de explicar el modo en que los buenos hábitos de seguridad benefician tanto a los empleados como a la empresa, al igual que los malos hábitos les causan problemas a ambos. Entre los beneficios se cuentan las redes que funcionan sin complicaciones y permiten a los empleados cumplir con su trabajo de forma satisfactoria. Finalmente, esto contribuye al incremento general de la productividad de la compañía. “Básicamente, la seguridad equivale a una buena filosofía administrativa que, a su vez, se traduce en mejoras de todos los aspectos de la empresa”

Hodge, William y Lawrence (2003) tratando el tema de los cambios organizacionales de manera eficiente dicen:"Las personas necesitan estar informadas sobre los cambios o cualquier proceso que afecte su desempeño laboral. La resistencia, la confusión y la hostilidad se pueden minimizar con una comunicación clara y oportuna sobre la naturaleza y el impacto de los cambios propuestos. Estas comunicaciones pueden incluir reuniones, videos, documentos y sesiones informativas".

La comunicación constituye una de las mejores armas para lograr que los empleados de las empresas asuman sus obligaciones con responsabilidad y amor.

De la Cuesta (2003) destaca que: "Cuando se establece una correcta comunicación interna en la entidad, se facilita el trabajo en cuanto al logro del cambio necesario, utilizando propuestas y métodos flexibles, creativos y la participación masiva e inteligente, en pero de lograr un compromiso consciente y entusiasta para acometer la tarea con la participación de todos los miembros de la entidad". No obstante, debe evitarse por todos los medios, la imposición forzada del cambio propuesto, ya que no surgirán factores positivos, indispensables para obtener resultados satisfactorios.

"El convencimiento es la forma válida para lograr el apoyo mayoritario a los cambios propuestos, de modo que los trabajadores varíen también la forma de pensar y actúen con criterios propios, responsablemente y con un

comportamiento estable. Sólo la comunicación efectiva puede lograr esos resultados. Cuantas más personas se sientan ignoradas en el proceso de cambio, mayor será la fuerza de oposición al cambio. La comunicación disminuye la resistencia equilibrando los poderes y emociones en las discusiones con el personal involucrado". Según De la Cuesta (2003).

De la Cuesta (2003) dice también que "la comunicación persuasiva tiene como intención, además, lograr que las transformaciones sean aceptadas y asimiladas por los receptores. Es ahí donde aparece la posibilidad de desarrollar el cambio después de una libre estimación de beneficios y costos relacionados con dicho proceso". Y argumenta que Aristóteles definió el arte de la retórica, como la capacidad de persuadir para obtener la cooperación y la confianza de las personas. Es por ello que, en situaciones de cambios e implementación técnica, debe existir una elevada capacidad de comprensión de la información y la explicación de la lógica del cambio, que debe ser predominante.

2.7 Departamento de Recursos humanos, seguridad de la información y ética empleados.

Microsoft 2009) en su artículo la información un capital cada día más preciado señala que Recursos Humanos debe involucrarse con el departamento de seguridad de la información en los aspectos de seguridad que afectan directamente a los empleados, como por ejemplo actualizando reglamento

interno, contratos de trabajo y anticipándose a la capacitación de usuarios para tener un plan de “evangelización” permanente y de largo plazo.

El área de recursos humanos es idealmente, desde donde se toman las decisiones más importantes en materia de seguridad informática. De igual forma, y en la medida que recursos humanos participe en los aspectos contractuales, estableciendo cláusulas especiales en los contratos de trabajo de empleados críticos, coordinando con el asesor legal y realizando los trámites en la secretaria del trabajo, se podrá lograr una base contractual, para los casos en que se descubran empleados realizando actos indebidos o violando la seguridad de la información de la compañía.

La norma internacional ISO 17799 menciona en uno de sus dominios, que la seguridad en una empresa debe partir desde la etapa de reclutamiento de personas. Independientemente de las políticas y procedimientos internos de reclutamiento y selección de personal, se debe tener políticas de seguridad complementarias aplicadas al proceso antes mencionado, ya que los controles y validaciones impuestos, podrían evitar el ingreso de un hacker o persona que engañe desde el inicio a la compañía.

La violación de las políticas de seguridad de la empresa son una situación que requiere de un ambiente de obligatoriedad especificada a través de disposiciones y sanciones, es decir: las normas jurídicas de la empresa; pues la

violación de las políticas de seguridad en la empresa se constituye en una violación de la ética en la misma.

Dependiendo de la gravedad, malicia o perversidad de la violación, las sanciones pueden ser desde una llamada de atención, informar al empleado o hasta el despido. Corresponderá al departamento de seguridad Informática hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la empresa.

Una reflexión de Muñoz (2005) dice que “el derecho y la ética, en conjunto, son una herramienta que permite fortalecer la Implementación de estrategias de seguridad informática”. Referente a esto el autor dice lo siguiente:

> En el momento en que se determina que la seguridad informática es un tema que involucra a todos los miembros de una organización y no sólo a ciertos puestos específicos dentro de la misma. La ética se refleja en la responsabilidad de considerarse parte de un proceso que tiene como fin único el preservar y conservar la integridad y buen manejo de la información, frente al mundo actual lleno de tecnología y, por ende, de riesgos que comprometen a la información.
>
> En el momento en que son implementados los procedimientos estipulados en la legislación vigente, ya sea en los procesos como en los marcos normativos internos de las empresas. Podría señalarse que:

… el daño a la información (vista esta como un bien mueble) puede ser causa de una rescisión laboral – justificada –.

… la revelación de un secreto empresarial es un delito.

… el hecho de no contar con licencias en sus programas de cómputo puede afectarle con una multa a la empresa y al empleado.

… la firma electrónica avanzada le permitirá tener un ambiente legal seguro en sus transacciones realizadas a través de medios electrónicos.

Por otra parte después de reconocer la importancia de que los empleados tengan conocimiento de las políticas de seguridad, es importante señalar que los empleados también deben conocer de los aspectos éticos que representa la violación de las políticas de seguridad, convirtiéndose también en parte fundamental de la que deben estar conscientes.

Ahora bien, luego de haber analizado la información antes descrita, en el marco teórico, se procede a plantear la siguiente hipótesis de carácter correlativa:

"A mayor nivel de comunicación de las políticas de seguridad a los empleados, menor es la vulnerabilidad de la información importante de la empresa"

En el presente estudio se utilizarán las siguientes variables e indicadores:

VARIABLES	DIMENSIONES	INDICADORES
Seguridad de la información	Confidencialidad	Nivel de utilización de la información en la toma de decisiones. Nivel de reconocimiento de la confidencialidad por parte de los empleados.
	Integridad	Nivel de confianza de los ejecutivos en la información.
Implementación políticas seguridad	Comunicación	Nivel de conocimiento de los empleados.
	Nivel de implementación	Nivel de cumplimiento por los empleados.
	Flexibilidad	Nivel de imposición

METODOLOGIA

III. METODOLOGÍA

3.1 Tipo de estudio.

Según sus objetivos, el tipo de estudio que se presenta es de carácter descriptivo- asociativo. Consiste en una descripción de aspectos de la seguridad de sistemas que están relacionados con los empleados para que se pongan en ejecución en las empresas. También se establece un análisis de correlación entre la comunicación de las políticas de seguridad y la implementación de las mismas en la empresa.

3.2 Descripción de la Población y muestra.

La población en estudio es de 300 empleados y 10 Altos ejecutivos de los cuales se tomó una muestra del 10% de los empleados , equivalente a 30 , y cinco (5) Ejecutivos, al azar, de la alta gerencia de Extra-seguros**.**

Para obtener dicha muestra se utilizó el muestreo aleatorio por nivel jerárquico.

3.3 Diseño de investigación adoptado.

El diseño de la investigación es de carácter transversal, donde se analizó la situación del cumplimiento de las políticas de seguridad de la empresa en el tiempo actual.

3.4 Procedimientos de Observación y medición utilizados.

La recolección de la información se hizo por medio a la implementación de cuestionarios a empleados por nivel y una entrevista con un guión al encargado de administrar la seguridad de la información de la empresa.

Para la medición se tabularon los resultados en tablas Excel obteniendo con dichos resultados los porcentajes para determinar los resultados del estudio.

RESULTADOS
Y
DISCUSION

IV. RESULTADOS Y DISCUSIÓN

4.1 Perfil del caso de estudio.

Extra-Seguros, SA. es una empresa de seguros de la República Dominicana, con muchos años de experiencia, que pertenece a uno de los grupos financieros más grandes y confiables del país. Ofrece sus servicios desde diferentes puntos estratégicos a todo el territorio nacional y sus productos están enfocados a pólizas de seguros para automóviles, edificaciones y personas (no ARS).

Esta empresa tiene una amplia gama de productos que con dedicación y estrategias de sus ejecutivos y empleados, han hecho la diferencia respecto a la competencia.

En los últimos años Extra-Seguros, SA. ha realizado muchos cambios de estrategias para mantener su posición y ganar ventajas en el mercado Asegurador Dominicano. Cada una de las metas establecidas en la empresa está enfocada hacia la satisfacción de sus clientes.

En la actualidad la empresa cuenta con 300 empleados y 10 Ejecutivos de la Alta Dirección. Extra-Seguros, SA. trabaja continuamente para mejorar su cultura organizacional. Sus empleados son el soporte esencial para el logro de los objetivos y así ganar ventajas competitivas y mantenerse en la vanguardia de los tiempos. La relación *Bienestar Empleado – Satisfacción Cliente– Resultados empresa* es el enfoque de la empresa en la actualidad. La empresa trabaja la

cultura de servicios con los empleados, ya que entiende que empleados identificados con las metas de la empresa, es la única forma de crear el camino hacia el logro de su visión, ser la mejor compañía de seguros del país reconocida por sus servicios.

La estructura de la empresa está distribuida de forma organizada por unidades de negocios, departamentos de apoyo y de operaciones. Dentro de la estructura existe una Subgerencia para la Administración de la seguridad de la información que está ubicada en el organigrama por debajo de la gerencia de Soporte técnico y base de datos en la vicepresidencia de tecnología.

El área de la Administración de la seguridad de la información es la responsable de lograr que la información de la empresa se mantenga libre de daños para que siempre se encuentre confiable, disponible e íntegra para el uso de la misma por sus empleados en el manejo del servicio y para los ejecutivos en la toma de decisiones.

Esta área de Extra-seguros SA, se encuentra en proceso de organización debido a procesos de grandes cambios por los que ha pasado la empresa. En la actualidad tiene definido un manual de políticas preliminar que ha colocado en la intranet para el uso general de los empleados de la empresa.

Extra-seguros SA, posee mucha tecnología para garantizar la seguridad de la información, pero aún no ha logrado que todos los miembros de la empresa

hagan suyos la seguridad, a sabiendas de que son los empleados los que constituye la mayor vulnerabilidad de la información como se argumentó en el marco teórico de esta investigación.

4.2 Resultados caso de estudio: EXTRA-SEGUROS SA.

Partiendo de la información suministrada por el Administrador de la Seguridad de la información de Extra-Seguros en entrevista realizada, se puede decir que la seguridad aplicada hasta el momento en la empresa es puramente restrictiva, es decir, aplicando restricciones por medio a la tecnología en los diferentes puntos débiles definidos por la empresa de forma obligatoria.

El Administrador de Seguridad de la información está consciente de que existe un descontento actual en los empleados, por las políticas implementadas en la empresa; además sabe que los empleados no conocen de la existencia del manual de políticas de seguridad y los que lo conocen nunca lo han leído. Muchos ni siquiera conocen el impacto ético que representa la violación de las políticas de seguridad para una empresa.

Un ejemplo comentado por el Administrador de la seguridad en la empresa es el caso de la restricción del uso del internet y deshabilitación de puertos USB de la mayoría de las computadoras de los empleados. “Los programadores se quejan porque dicen que la restricción en el internet afecta su productividad, pues muchas veces necesitan buscar información sobre aspectos que le impiden

continuar con su trabajo. Y aunque hemos buscado alternativas, colocando una Laptop para esos casos, ellos continúan con sus quejas".

El departamento de seguridad de la información lleva estadísticas de las violaciones de los empleados en la medida que sea posible llevarlas, como son el uso del internet en cuanto a tiempo y movimientos de páginas, monitoreo de correos, accesos a sistemas, a servidores, entre otros. Y señala que las violaciones de seguridad de la información se dan a todos los niveles de la organización, aunque en mayor porcentaje en niveles bajos.

El administrador de la seguridad de la información expresó que a pesar de todas las restricciones aplicadas en la empresa por medio a las tecnologías, aún la información de la empresa es vulnerable, pues muchas de las medidas están sujetas a ser aplicadas por los empleados y no hay manera de controlarlo por medio a una herramienta. Como ejemplo de estas medidas están:

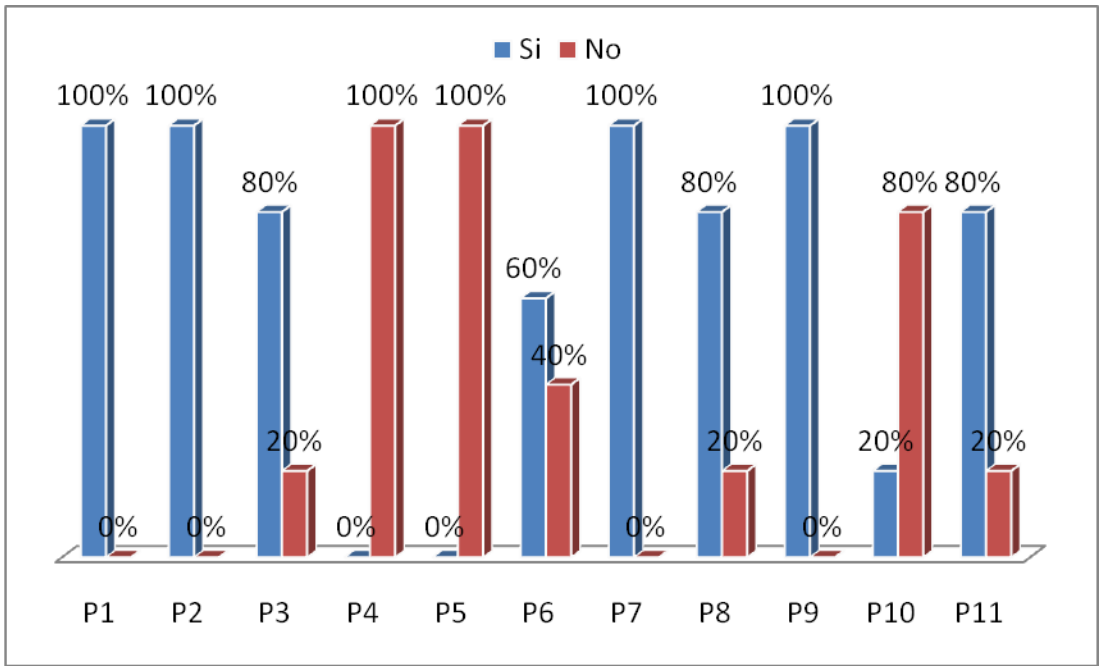
1. Uso correcto de las contraseñas, esto es que no la den a compañeros, ni la creen con códigos fáciles de adivinar por cualquier persona.
2. Uso correcto del correo electrónico. Los correos en cadenas están prohibidos para evitar cargar la red con informaciones que no significan nada en el trabajo que realizan.

Muchas veces no mantienen depurado su correo, si no que almacenan en él informaciones personales y pudieran utilizarlo para sacar información confidencial de la empresa, entre otros.

3. Bloqueo de las PCs. Los empleados no deben dejar sus PCs encendidas sin bloquear, pues puede que cualquier información sea tomada con su usuario, sin dejar rastro alguno.
4. Uso correcto de documentos importantes y confidenciales. Los empleados deben guardar en lugar seguro y con llaves.
5. Manejo correcto de la información llevada en Laptops de trabajo y en memorias USB.
6. Pasar antivirus a las memorias USB que hayan sido utilizadas fuera de la empresa, antes de introducirla en algunas de las computadoras que tienen acceso.
7. Uso correcto de la información de la empresa. Esto es no divulgarla cuando este fuera de ella.
8. Uso correcto de almacenamiento de archivos y de herramientas de la empresa para utilizarlos a manera personal, entre otras medidas.

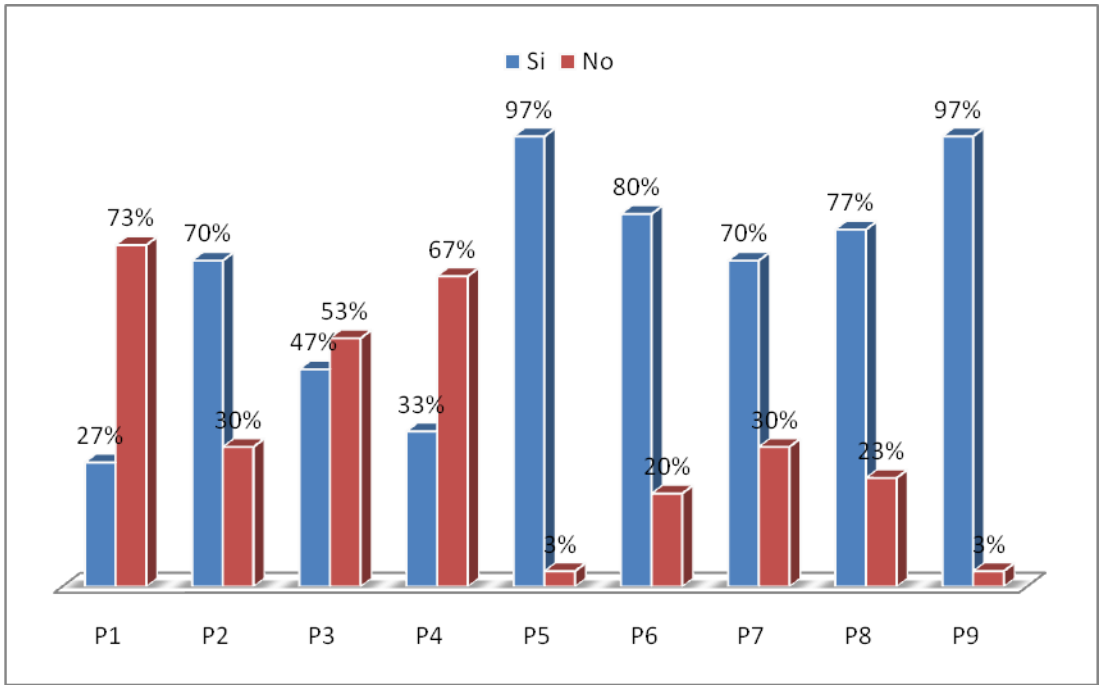
En cuanto a los cuestionarios realizados tanto a la Alta gerencia como los demás empleados se obtuvieron los siguientes resultados (por preguntas p1…p11) que se analizan de forma comparativa entre ambos niveles como sigue:

Gráfico 2. Resultados porcentuales Cuestionarios Alta Gerencia



Fuente: Elaboración propia, Cuestionarios Alta Gerencia Extra-Seguros 2009

Gráfico 3. Resultados porcentuales Cuestionarios Empleados



Fuente: Elaboración propia, Cuestionarios empleados Extra-Seguros 2009

a. La Alta gerencia utiliza y considera que la información de los sistemas de la empresa, es confiable y siempre está disponible en un 100% (P1 y P2).

b. El 80% de los Ejecutivos (P3) conocen de la existencia del manual de las políticas de seguridad de la empresa, mientras el 73% de los empleados (P1) desconocen este manual. Lo que se puede decir que la alta gerencia normalmente tienen un conocimiento más amplio de las razones de sus deberes en la empresa, debido a su nivel y en cuanto a los demás empleados se puede deducir que ha habido poca comunicación de parte del área de administración sobre la importancia de este documento en la empresa.

c. El 100% de los ejecutivos (P4) consideran que las políticas de seguridad de la información no afectan su desempeño en la empresa, mientras que el 70% de los empleados (P2) si consideran que afectan su desempeño laboral.

d. El 100% de los ejecutivos (P5) no perciben las medidas de seguridad establecidas en la empresa como una molestia, mientras el 53% de los empleados (P3) si la perciben como molestia y si pudieran evadirla lo hicieran.

e. El 60% de los ejecutivos (P6) consideran la aplicación de las políticas de seguridad como parte de su responsabilidad laboral, mientras que el 67% de los empleados (P4) no la consideran parte de su responsabilidad.

f. El 100% de los ejecutivos (P7) y el 97% de los empleados (P5) saben que la información que manejan en la empresa es confidencial y que no debe ser divulgada fuera de ella.

g. El 80% de los ejecutivos (P8) y de los empleados (P6) conocen el impacto ético que tiene la violación de las políticas de seguridad de la empresa.

h. El 100% de los ejecutivos (P9) y el 70% de los empleados (P7), reconocen que las políticas de seguridad que conocen en la empresa son de fácil aplicación.

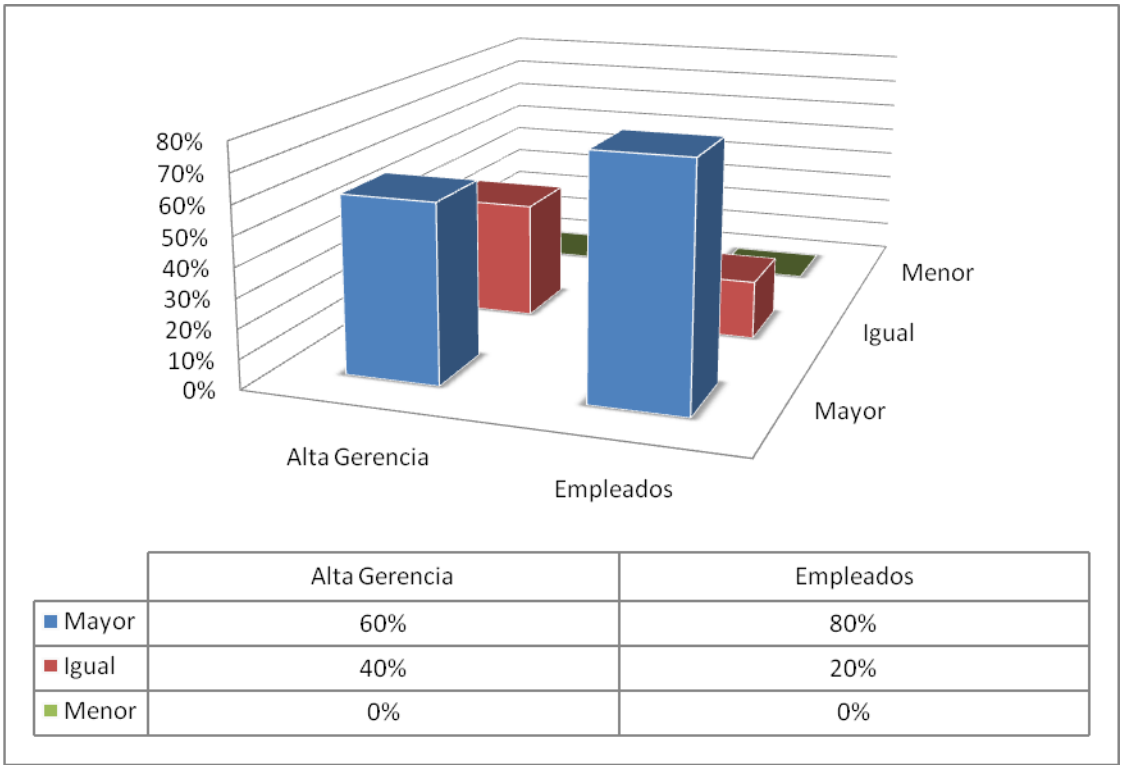
i. El 80% de los ejecutivos (P10) entienden que no necesitan más información sobre las políticas de la seguridad, mientras que el 77% de los empleados (P8) entienden que es necesario conocer más información.

j. El 80% de los ejecutivos (P11) y el 97% de los empleados (P9) consideran que debe haber más comunicación de las políticas de seguridad a los empleados en la empresa.

k. En cuanto al grado de compromiso de los empleados de Extra-Seguros SA., una vez fueran informados sobre el objetivo de cada política de seguridad de la empresa se tiene que el 80% de los empleados (P10) y el 60% de los

ejecutivos (P12) tendrían un grado mayor de compromiso, como se puede observar en el gráfico 3 que se presenta a continuación.

Gráfico 4.
Nivel de compromiso una vez informados sobre las políticas de seguridad de la información



	Alta Gerencia	Empleados
Mayor	60%	80%
Igual	40%	20%
Menor	0%	0%

Fuente: Elaboración propia, pregunta alta gerencia (12) y empleados (10), Extra-Seguros 2009

4.3 Análisis resultados, Caso Extra-Seguros.

Analizando los resultados del cuestionario a los empleados y la entrevista hecha al administrador de la seguridad de la información de Extra-Seguros se puede decir que:

- ✓ La información de la empresa es considerada íntegra y confiable por los ejecutivos, ya que están muy conformes con la seguridad implementada en la empresa y los empleados dicen conocer que la información de la empresa es confidencial.

  Es importante señalar que el hecho de que la información sea confiable o no, sigue siendo un punto de vulnerabilidad; pues depende de la honestidad y la ética de los empleados, el que sean cumplidas o no las políticas de seguridad establecidas.

- ✓ La interrelación entre el departamento de Seguridad de la información y los empleados no ha sido la más apropiada; pues la mayoría de los empleados desconocen el manual de políticas de seguridad, consideran que las políticas de seguridad son un estorbo en su desempeño laboral y no entienden que el cumplimiento de dichas políticas forman parte de sus funciones en la empresa.

- ✓ La mayoría de los empleados de Extra-Seguros conocen del impacto ético que representa el incumplimiento de las políticas de seguridad en la empresa. Una de las razones por las que se puede decir que la información de la empresa es considerada aun íntegra y confiable.

- ✓ La comunicación respecto a las políticas de seguridad en la empresa ha sido deficiente en los niveles bajos; pues la mayoría de los empleados entienden

que necesitan más información del por qué de las políticas implementadas y entienden además que la empresa debe tener más comunicación con ellos.

- ✓ Las políticas establecidas en la empresa son poco flexibles, de total imposición, necesitan suavizarse o por lo menos ser comprendidas por los afectados, para su mejor aplicación.

- ✓ Los empleados de Extra-seguros tienen poco grado de conocimiento sobre las políticas de seguridad, lo que ha impactado negativamente en la confidencialidad e integridad de la información, pues según comentaba el administrador de la seguridad de la información, son muchas las violaciones cometidas a diarios por los empleados de todos los niveles, a las que ha tenido que optar por aplicar muchas medidas restrictivas, como única manera viable hasta el momento, para garantizar menos vulnerabilidad en la seguridad de la información en cuanto a integridad y disponibilidad.

- ✓ El administrador de la seguridad de la información en la empresa sabe que necesita aplicar nuevas medidas que le ayuden a disminuir la vulnerabilidad de la información y a lidiar con todos los inconvenientes que se le presentan al tratar de ejercer su función.

CONCLUSIONES

V. CONCLUSIONES

La información es el principal activo que tienen las empresas. Por medio al procesamiento de la información, las compañías crean valor, ayudando ésto a que logren sus objetivos y por esta razón debe ser muy bien protegida.

Las empresas establecen medidas o políticas de seguridad que documentan en los denominados “Manuales de políticas de seguridad” y que deben ser de conocimiento y aplicación por parte de todos los empleados. Siendo responsabilidad del Administrador de la seguridad de la información el comunicar y sensibilizar al personal respecto a dichas medidas.

El administrador de la seguridad de la información debe encargarse de mantener comunicados a los empleados del impacto que tendrá una nueva medida de seguridad en su actividad diaria, cómo afectará su trabajo y debe convencer a los empleados de que esa incomodidad es el precio de proteger la información; pues muchas de las brechas de seguridad se dan por simple desconocimiento. Como dicen Hodge, William y Lawrence (2003) ”Las personas necesitan estar informadas sobre los cambios o cualquier proceso que afecte su desempeño laboral. La resistencia, la confusión y la hostilidad se pueden minimizar con una comunicación clara y oportuna sobre la naturaleza y el impacto de los cambios propuestos”.

La violación de las medidas de seguridad conllevan un impacto ético que debe establecerse en cláusulas especiales en los contratos de trabajo de los empleados, coordinando con el asesor legal y realizando los trámites en la secretaria del trabajo, esto para los casos en que se descubran empleados realizando actos indebidos o violando la seguridad de la información de la compañía. La violación de las políticas de seguridad puede implicar desde una simple sanción hasta el despido sin prestaciones de un empleado, dependiendo de la gravedad del delito.

El caso de Extra-seguros es que la información aún es entendida como confiable para los ejecutivos; pero la realidad para el administrador de la seguridad de la información es que los empleados de todos los niveles violan la seguridad y aunque hasta el momento tiene control sobre estas violaciones, puede llegar un momento en que se le escapen de las manos. Pues con el avance de la tecnología, se crean muchas brechas, generándose así mayores riesgos en la seguridad de la información de la empresa.

Los empleados de las empresas representan el mayor porcentaje de vulnerabilidad de la información, siendo la mayoría de las veces poco conscientes de la importancia de conocer y aplicar dichas políticas. Por esto aumentar el grado de conocimiento de los empleados sobre las políticas de seguridad de la información, impacta de manera positiva en la confiabilidad e integridad de la información, ya que es la mejor forma de lograr que el

problema del área de seguridad de la información se convierta en el problema de todos. Lográndose así, mayor eficiencia en el cuidado de la información.

5.1 Recomendaciones.

Las empresas deben Implementar campañas de sensibilización a los empleados de forma periódica, sobre las políticas de seguridad.. Estas actuaciones se deberán llevar a cabo mediante la convocatoria de seminarios o presentaciones, exposición de películas o vídeos, colocación de carteles, distribución de boletines internos, entrega de premios por actividades sobre seguridad, envío de notificaciones electrónicas, actividades relacionadas con seguridad, así como cualquier otra que se estime oportuno. Además deben:

- ✓ Crear un procedimiento para la implementación de las nuevas políticas en la empresa, que contenga la divulgación de las mismas, como parte indispensable para dicha implementación.

- ✓ Incluir en los procedimientos de Recursos Humanos , los vínculos que existen entre este departamento y el de Seguridad de la información, tomando en cuenta que la seguridad y su impacto ético debe ser punto importante desde el reclutamiento, la selección , la inducción …hasta las sanciones por violaciones de las políticas.. Véase Apéndice 7. Ejemplo de Procedimiento de reclutamiento de personal ..

- ✓ Realizar censos o encuestas al personal sobre aspectos puntuales del uso de buenas prácticas en el manejo y uso de la plataforma tecnológica y los recursos de información.

- ✓ Crear un buzón de sugerencias y/o realizar reuniones de lluvias de ideas para recibir las opiniones de los empleados respecto a las políticas implementadas que afectan su desempeño, escuchar sus inquietudes y buscar soluciones óptimas a los inconvenientes presentados.

REFERENCIAS BIBLIOGRAFICAS

REFERENCIAS BIBLIOGRÁFICAS

Benson, Christopher (2000). Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft © Solutions. Extraído el 18 de Julio del 2009 desde http://www.segu-info.com.ar/politicas/

Cisco Systems inc (2008). Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados. Extraído el 11 de Julio 2009 desde: http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf?sid=177824_10

De la Cuesta, Guillermo (2007). Comunicación eficiente: parte esencial en los cambios empresariales. Extraído el 11 de Julio 2009 desde http://www.opciones.cu/leer.asp?idnuevo=315624

Evans, James R. y Linsdsay, William M. (2008). Administración y control de la calidad 7ma ed. Medición del desempeño y Administración de la información estratégica. 392.

Hodge, B. J., William P. Anthony, Lawrence M. Gates (2003). Teoría de la organización. Un enfoque estratégico. 6Ta ed. Cap.13 Innovación, Cambio estratégico y aprendizaje organizativo. Facilitar el cambio, las comunicaciones,p-385.

Huerta, Antonio Villalón (2000). Seguridad en Unix y redes. (Versión 1.2). Capítulo 16-Página 259. Extraído el 11 de Julio 2009 desde http://www.segu-Info.com.ar/politicas/polseginf.htm

Izquierdo, Víctor (2009). Mejor formación y herramientas para medir el ROI. Extraído desde http://seguinfo.wordpress.com/category/politicas/

Muñoz Torres, Ivonne V (2005). Aspectos Legales y Éticos de la Seguridad Informática©Una reflexión local y global. Extraído el 11 de Julio 2009 desde http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/MunozTorres.pdf

Microsoft.(2009) la información: un capital cada vez más preciado Extraido el 01-ago-2009. Desde la web disponible en http://www.microsoft.com/conosur/proseguridad/informacion.aspx

Oz, Effy (2008). Administración de los sistemas de información, 5ta ed. Riesgos, seguridad y recuperación ante desastres. Riesgos para los sistemas de información. Riesgos para los datos y las aplicaciones. Pp.444, 463

Pallavicini, César (2009) riesgos si no participa recursos humanos . El Mercurio Norma ISO 1779. Extraído el 01 agosto 2009 desde http://www.seguridadinformacion.cl/articulos/riesgos-sino-participa-rrhh.html

Plamondon, Scout (2006**).** El peor riesgo para la seguridad puede resultarle útil. Cómo ayudar a sus empleados a adquirir mejores hábitos de seguridad. Extraído el 11 de Julio 2009 desde http://www.microsoft.com/spain/medianaempresa/securityrisk.mspx

Spafford, Gene (2000). "Manual de seguridad en redes". ArCERT. Argentina. http://www.arcert.gov.ar. Extraído el 11 de Julio 2009 desde http://www.segu-Info.com.ar/politicas/polseginf.htm

Tirado Juan M. (2009). La-responsabilidad-de-los-usuarios-finales-en-la-cadena-de-protección. Extraído el 11 de Julio 2009 desde http://mundopc.net/articulos

APENDICES

Apéndice 1. Guión de Entrevista (Administrador Seguridad de Información)

1. ¿Existe un manual de políticas de seguridad de la información en Extra-Seguros de fácil acceso a los empleados?
2. ¿Me puede citar algunas de las medidas que dependan del empleado para ser aplicadas en la empresa?. Y comente acerca de su aplicación actualmente.
3. ¿Qué porcentaje de empleados conoce este manual? Entiende que los que lo conocen lo están aplicando?
4. ¿Cómo considera usted que se sienten los empleados con las políticas establecidas por la empresa?
5. ¿Su departamento lleva un control de los registros de monitoreo de transacciones? En este control se pueden determinar las violaciones de seguridad por parte de los empleados?
6. ¿Si guarda registro de las violaciones, existen violaciones a todos los niveles de la estructura o a que nivel?. Más o menos en que porcentaje?
7. ¿Conocen los empleados del impacto ético que implica la violación de las políticas establecidas en el manual?. Coménteme
8. ¿Qué medidas ha implementado hasta el momento, para que los empleados cumplan las políticas?
9. ¿Sería posible que me muestre el Manual de las políticas para revisar su contenido con más detalle?

Apéndice 2. Cuestionario a Empleados

1. ¿Conoce usted de la existencia de un manual de políticas de seguridad en la empresa?

   ◉ **SI** ○ **NO**

2. ¿Las políticas de seguridad establecidas por la empresa afectan su desempeño laboral?

   ○ **SI** ○ **NO**

3. ¿Percibe las medidas de seguridad restrictivas (ej: restricción del internet) como una molestia que si usted tuviera la oportunidad la evadiera?

   ○ **SI** ○ **NO**

4. ¿En su labor en la empresa, considera estas políticas como parte de su responsabilidad?

   ○ **SI** ○ **NO**

5. ¿Sabía Usted que la información que maneja es confidencial, por lo que no debe ser divulgada por ningún motivo?

   ○ **SI** ○ **NO**

6. ¿Tiene conocimiento del impacto ético (Valores, rigores, principios internos) que conlleva la violación de las políticas de seguridad?

   ○ **SI** ○ **NO**

7. ¿Considera de fácil aplicación o cumplimiento las políticas de seguridad que conoce en la empresa?

   ○ **SI** ○ **NO**

8. ¿Considera que necesita mayor información o motivación sobre el por qué de las políticas implementadas?

   ○ **SI** ○ **NO**

9. ¿Considera que debe haber mayor comunicación de las políticas hacia los empleados?

   ○ **SI** ○ **NO**

10. ¿Cuál sería su grado de compromiso una vez informado sobre el objetivo de cada política de seguridad?

    ○ Mayor ○ Igual ○ Menor

Apéndice 3. Cuestionario Ejecutivos Alta Gerencia

1. ¿Utiliza la información de los sistemas informáticos para tomar decisiones importantes para la empresa?
   ○ **SI** ○ **NO**
2. ¿La información está siempre disponible y es confiable?
   ○ **SI** ○ **NO**
3. ¿Conoce usted de la existencia de un manual de políticas de seguridad en la empresa?
   ○ **SI** ○ **NO**
4. ¿Considera que las políticas de seguridad establecidas por la empresa afectan su desempeño laboral?
   ○ **SI** ○ **NO**
5. ¿Percibe las medidas de seguridad restrictivas (ej: restricción del internet) como una molestia que si usted tuviera la oportunidad la evadiera?
   ○ **SI** ○ **NO**
6. ¿En su labor en la empresa, considera estas políticas como parte de su responsabilidad?
   ○ **SI** ○ **NO**
7. ¿Sabía Usted que la información que maneja es confidencial, por lo que no debe ser divulgada por ningún motivo?
   ○ **SI** ○ **NO**
8. ¿Tiene conocimiento del impacto ético (Valores, rigores, principios internos) que conlleva la violación de las políticas de seguridad?
   ○ **SI** ○ **NO**
9. ¿Considera de fácil aplicación o cumplimiento las políticas de seguridad que conoce en la empresa? ○ **SI**
   ○ **NO**
10. ¿Considera que necesita mayor información o motivación sobre el por qué de las políticas implementadas?
    ○ **SI** ○ **NO**
11. ¿Considera que debe haber mayor comunicación de las políticas hacia los empleados?
    ○ **SI** ○ **NO**
12. ¿Cuál sería su grado de compromiso una vez informado sobre el objetivo de cada política de seguridad?
    ○ Mayor ○ Igual ○ Menor

Apéndice 4. Resultado encuestas empleados

Preguntas	SI	NO
1.-¿Conoce usted de la existencia de un manual de políticas de seguridad en la empresa?	8	22
2.-¿Considera que las políticas de seguridad establecidas por la empresa afectan su desempeño laboral?	21	9
3.-¿Percibe las medidas de seguridad restrictivas (ej: restricción del internet) como una molestia que si usted tuviera la oportunidad la evadiera?	14	16
4.- ¿En su labor en la empresa, considera estas políticas como parte de su responsabilidad?	10	20
5.-¿Sabía Usted que la información que maneja es confidencial, por lo que no debe ser divulgada por ningún motivo?	29	1
6.-¿Tiene conocimiento del impacto ético (Valores, rigores, principios internos) que conlleva la violación de las políticas de seguridad?	24	6
7.-¿Considera de fácil aplicación o cumplimiento las políticas de seguridad que conoce en la empresa?	21	9
8.-¿Considera que necesita mayor información o motivación sobre el por qué de las políticas implementadas?	23	7
9.-¿Considera que debe haber mayor comunicación de las políticas hacia los empleados?	29	1

	MAYOR	IGUAL	MENOR
10-¿Cuál sería su grado de compromiso una vez informado sobre el objetivo de cada política de seguridad?	24	6	0

Apéndice 5. Resultado encuestas Alta Gerencia

Preguntas	SI	NO
1.-¿Utiliza la información de los sistemas informáticos para tomar decisiones importantes para la empresa?	5	0
2.-¿La información está siempre disponible y es confiable?	5	0
3.-¿Conoce usted de la existencia de un manual de políticas de seguridad en la empresa?	4	1
4.-¿Considera que las políticas de seguridad establecidas por la empresa afectan su desempeño laboral?	0	5
5.-¿Percibe las medidas de seguridad restrictivas (ej: restricción del internet) como una molestia que si usted tuviera la oportunidad la evadiera?	0	5
6.- ¿En su labor en la empresa, considera estas políticas como parte de su responsabilidad?	3	2
7.-¿Sabía Usted que la información que maneja es confidencial, por lo que no debe ser divulgada por ningún motivo?	5	0
8.-¿Tiene conocimiento del impacto ético (Valores, rigores, principios internos) que conlleva la violación de las políticas de seguridad?	4	1
9.-¿Considera de fácil aplicación o cumplimiento las políticas de seguridad que conoce en la empresa?	5	0
10.-¿Considera que necesita mayor información o motivación sobre el por qué de las políticas implementadas?	1	4
11.-¿Considera que debe haber mayor comunicación de las políticas hacia los empleados?	4	1

	MAYOR	IGUAL	MENOR
12.-¿Cuál sería su grado de compromiso una vez informado sobre el objetivo de cada política de seguridad?	3	2	0

Apéndice 6. Glosario de términos

Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Base de datos: es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. En la actualidad, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), que ofrece un amplio rango de soluciones al problema de almacenar datos.

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Gadgets: es un dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso. Los gadgets suelen tener un diseño más ingenioso que el de la tecnología corriente.

Impacto: medir la consecuencia al materializarse una amenaza.

Malware: es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas.

Ordenador: También denominado computador, es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

Pendrives: (USB flash drive) es un pequeño dispositivo de almacenamiento que utiliza memoria flash para guardar la información. Estas memorias son resistentes a los rasguños (externos) al polvo, y algunos al agua- que han afectado a las formas previas de almacenamiento portátil-, como los disquetes, discos compactos y los DVD.

Redes de comunicación: Redes de comunicación, no son más que la posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios.

Riesgo: posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.

Seguridad informática: consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

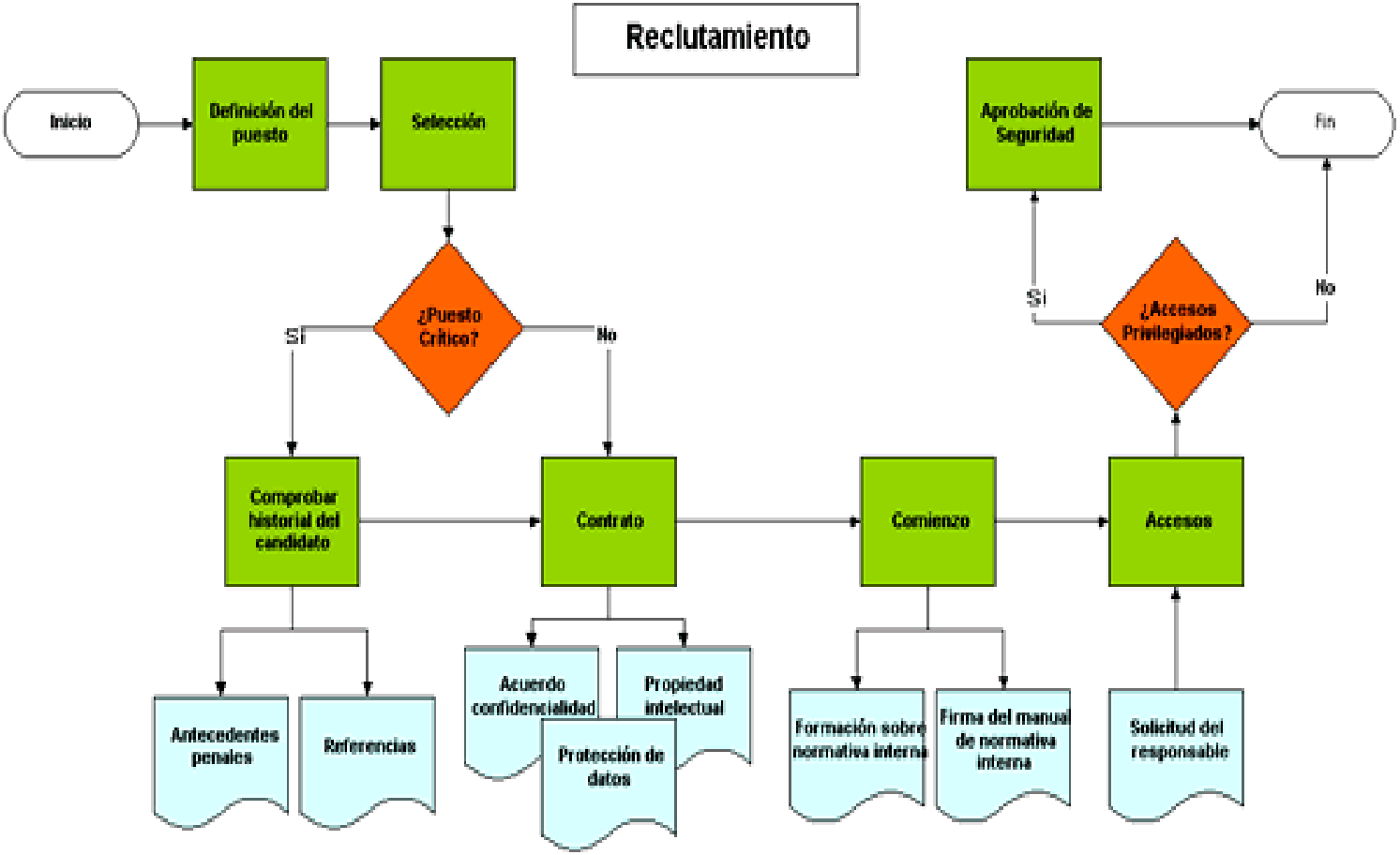
Servidores: Una computadora en la que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes, tanto si se trata de un ordenador central (*mainframe*), un miniordenador, un ordenador personal, una PDA o un sistema integrado;

Virus informáticos: es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Estas definiciones fueron extraídas del portal de Wikipedia en la Web.

Apéndice 7. Procedimiento de reclutamiento de personal



Apéndice 8. Ejemplo de procedimiento de Análisis de gestión de riesgos.