ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Planificación de Políticas de Seguridad".

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentada por

MARÍA ESPERANZA DÍAZ VALLE

JOSÉ ANGEL NAVARRO MASPONS

Guayaquil - Ecuador

2011

AGRADECIMIENTO

A Dios, porque sin su bendición no hubiese sido posible la realización de este proyecto, a mis madres: Zoila y Julia y a mi padre Celso por toda la ayuda y apoyo que me brindaron durante toda mi vida estudiantil y finalmente a mis maestros por la enseñanza que me han brindado y fueron razón de inspiración para permitirme culminar con éxitos esta obra.

María E. Díaz Valle

Por el apoyo brindado durante todos estos años de estudios que me han permitido culminar esta primera etapa en mi carrera profesional mis más sinceros agradecimientos, a mis padres Daisy y José. A los docentes que con sus palabras y ejemplos fueron fuente de inspiración y guía para seguir adelante. Y a mis amigos que me apoyaron con sus ideas y aliento durante los momentos difíciles en el desarrollo de este proyecto.

José Angel Navarro Maspons

DEDICATORIA

A la memoria de mi abuelita Raquel, que sin duda alguna en el sitio que se encuentre junto a Dios, está muy orgullosa por mi éxito conseguido y a quien llevo siempre presente en mi corazón.

María E. Díaz Valle

Dedico este trabajo resultado de esfuerzo y dedicación a mi familia por sus palabras y buenos deseos que me brindaron todo este tiempo.

José Angel Navarro Maspons

TRIBUNAL DE SUSTENTACIÓN

_____

ING. IGNACIO MARÍN GARCÍA, MSIS
PROFESOR DEL SEMINARIO
DE GRADUACIÓN

_____

ING. LENÍN FREIRE COBO, MSIG
PROFESOR DELEGADO
DEL DECANO

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesina, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL

(REGLAMENTO DE GRADUACIÓN DE LA ESPOL)

_____

MARÍA ESPERANZA DÍAZ VALLE

_____

JOSÉ ANGEL NAVARRO MASPONS

RESUMEN

El presente trabajo consiste en la planificación de las Políticas de Seguridad para Empresas de tamaño medio y que se dedican en especial a brindar algún tipo de servicio de telecomunicaciones.

Para el éxito en el desarrollo de este documento seguimos las recomendaciones que sugieren los estándares ISO/IEC 17799:2005, ISO/IEC 27000:2009, el manual de Políticas de Seguridad Informática- Mejores Prácticas Internacionales y otros adjuntos. Logrando así considerar todos los aspectos de seguridad que se deben analizar en las empresas y consiguiendo además orden y aceptación de las propuestas que exponemos.

Presentamos propuestas que ayudan a realizar una mejora continua de los documentos de Políticas de Seguridad que se han decidido aplicar y de como mejorar la manera en que se integran estas políticas en el ambiente laboral a través de un conjunto de sugerencias que cubren la manera en que deben aplicarse las políticas, darles seguimiento y lo más importante aún conseguir que el personal de la empresa acepte y cumpla con las Políticas.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

LISTA DE ABREVIATURA

DPTO.: Departamento

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional)

ISO: International Organization for Standarization (Organización Internacional para la Estandarización)

IT: Information technology (Tecnologia de la informacion)

PC: Ordenador Personal (Personal Computer)

PDCA: plan–do–check–act (PLAN-HACER-REVISAR-ACTUAR)

SGSI: Sistema de Gestión de la seguridad de la Información

GLOSARIO

Administrador de red: Administrador de red, especialista de red y analista de red se designan a aquellas posiciones laborales en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la administración de la red.

Antivirus: Dicho de un programa: Que detecta la presencia de virus y puede neutralizar sus efectos.

Audiencia: Número de personas que reciben un mensaje a través de cualquier medio de comunicación.

Auditores: Persona encargada de realizar los procesos de auditoria.

Auditoría: Una visión formal y sistemática para determinar hasta qué punto una organización está cumpliendo los objetivos establecidos por la gerencia, así como para identificar los que requieren mejorarse.

Controles: Son dispositivos o mecanismos usados para guiar la operación de una máquina, aparato, sistema o un proceso.

Dictamen: Opinión y juicio que se forma o emite sobre algo.

Directriz: Conjunto de instrucciones o normas generales para la ejecución de algo.

Documentos auditables: Documentos que son parte de un proceso de auditoria.

Estándar: Que sirve como tipo, modelo, norma, patrón o referencia.

Evaluación de riesgo: Es la ciencia que estudia la comprensión y la medida de los peligros así como la exposición y, en última instancia, los riesgos asociados. Se trata, por necesidad, de una ciencia interdisciplinar.

Firewalls: Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Firmas de declaración de conformidad: Método de comprobación y registro sobre la aceptación de lo que se declara.

Gerencia: Se denomina al conjunto de empleados de alta calificación que se encarga de dirigir y gestionar los asuntos de una empresa.

Gestión: Acción y efecto de administrar.

Gusanos: Programa que se reproduce por sí mismo, que puede viajar a través de redes utilizando los mecanismos de éstas y que no requiere respaldo de software o hardware para difundirse.

Lineamiento: Es una tendencia o dirección sobre la forma en la que se debe resolver una tarea.

Matriz: Molde de cualquier clase con que se da forma a algo.

Motores de búsqueda: Es un sistema informático que busca archivos almacenados en servidores web.

Multiusuario: Se refiere a un concepto de sistemas operativos, pero en ocasiones también puede aplicarse a programas de ordenador de otro tipo (e.j. aplicaciones de base de datos). En general se le llama multiusuario a la característica de un sistema operativo o programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente (tanto en paralelismo real como simulado).

Norma: Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.

Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Procedimiento: Define la manera en que se debe realizar una tarea.

Proceso técnico – administrativo: que involucra la participación tanto del área técnica como de la administrativa.

Red: Conjunto de ordenadores o de equipos informáticos conectados entre sí que pueden intercambiar información.

Seguridad: Podemos entender como seguridad una característica de cualquier sistema (informático o de información) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Sistema informático: Un sistema informático como todo sistema, es el conjunto de partes interrelacionadas, hardware, software y de Recurso Humano (humanware). Un sistema informático típico emplea una computadora que usa dispositivos programables para capturar, almacenar y procesar datos.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Troyanos: Un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Usuarios: Dicho de una persona: Que tiene derecho de usar de una cosa ajena con cierta limitación.

Virus: Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada.

INTRODUCCIÓN

A medida que la infraestructura de las empresas crece, se producen un aumento del personal y divisiones departamentales. Esto presenta nuevas dificultades para proteger la información y mantener correctas relaciones laborales entre el personal. Surge así la importancia de implementar mecanismos de seguridad que permitan proteger y dar un orden a la continua expansión de la infraestructura a través del tiempo. El correcto funcionamiento del crecimiento de los sistemas empresariales va ligado de una buena definición de normas, lineamientos, procedimientos y controles que permitan cuidar y alcanzar los intereses gerenciales. Con la finalidad de definir estas guías adecuadas, se presenta en este documento un manual de reglamentos conocido como “Políticas de Seguridad”. Las políticas de seguridad brindan a la empresa la oportunidad de lograr alcanzar los estándares internacionales tanto en seguridad como calidad de sus servicios ofrecidos, otorgando así una buena imagen que permite incrementar la confianza y aceptación de sus clientes. Quedando claro entonces, la necesidad inmediata de definir un esquema de políticas que aseguren a la empresa de los riesgos que pudieran presentarse.

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

Toda empresa necesita de políticas, normas o procedimientos que le permitan llevar un mejor control en las acciones que realiza. Pero, para esto es primordial identificar las áreas en donde se va implementar la seguridad, antes de dar inicio a la escritura del documento. El identificar las áreas claramente, nos permitirá redactar mejor las políticas, porque, desde un principio, las estaremos enfocando directamente al lugar donde se va a dar la seguridad, sabiendo con lo que ya se cuenta y como se lo va a mejorar. Continuaremos luego aclarando conceptos importantes que se deben conocer para conseguir un mayor entendimiento y sobre todo la visualización del alcance que se puede llegar a obtener en temas de seguridad al contar con un adecuado documento de políticas.

1.1. ÁREAS PRIMORDIALES DE LA SEGURIDAD

Hay que tener en cuenta que no siempre es necesario o posible para las empresas cubrir todas sus áreas que se puedan identificar con un elevado nivel de seguridad. Las áreas a seleccionar y el nivel de seguridad correspondiente dependerá en gran medida de los intereses primordiales que presenten la gerencia. La clasificación de las áreas de seguridad es:

- **Seguridad Física y Dispositivos:**

  La seguridad efectiva tanto de clientes como servidores requiere conseguir un equilibrio entre el grado de protección y el nivel de disponibilidad, que en muchos casos estos dos aspectos se entiende como contrapuestos. Para lograr esto, los encargados de la seguridad pueden incluir para su protección: la desactivación de servicios, eliminación de ciertos derechos de usuario, mantenimiento al día del sistema operativo y el uso de productos antivirus y de firewalls distribuidos. La tecnología se ha ido multiplicando rápidamente hoy en día, brindando al usuario las oportunidades de conectarse a los sistemas informáticos de la empresa, desde el PC de escritorio tradicional hasta los modernos teléfonos móviles de última

generación; esta razón ha dado nuevos escenarios y necesidades de seguridad a su empresa, con respuestas rápidas y específicas.

- **Gestión de Riesgo:**

  El manejo de riesgos se centra en los posibles problemas de seguridad que se puedan dar por causas físicas o legales; por ejemplo: desastres naturales o incendios, accidentes, muertes o demandas. Por eso el implantar políticas en base a evaluaciones de riesgos se podrán evitar problemas y pérdidas muy graves en las empresas a través del tiempo.

- **Seguridad de Red y Perimetral:**

  Una red mal configurada, sin un diseño basado en estándares con una protección física inadecuada, puede presentarse como un factor elevado de riesgo para la seguridad de la información. Los administradores de la red tienen que asegurar la seguridad física de sus componentes para impedir los accesos no autorizados. Impedir el acceso no autorizado de personas sobre áreas de interés, mediante señales de aviso y aclaraciones bien definidas, resultan una solución clave para el incremento de la seguridad y obtención de orden y comodidades para todo el personal en las empresas.

- **Seguridad de Software y sus aplicaciones:**

  Administradores de sistemas deben están familiarizados con los virus, gusanos o troyanos que son los ataques más comunes a la red. El conocer sus características y consecuencias, le ayudara a dotarse de herramientas y métodos de protección y eliminación, brindando la mejor seguridad a la red de la empresa.

  El control del correo electrónico sigue siendo un problema importante en tiempo y recursos, ya que siendo éste regularmente un portador de gusanos y virus, se considera una importante amenaza para la seguridad de la PC. Pero, con el avance de la tecnología hoy en día se pueden evitar correos no deseados, virus y otras amenazas que perjudiquen a la red.

- **Seguridad en la Información:**

  Hay que tener en cuenta que los sistemas contienen información muy importante y esencial, por lo cual requiere protección contra la modificación o divulgación no autorizada de estos recursos. Así mismo, estos proporcionan servicios que deben estar disponibles en el momento que se estime conveniente y sean requeridos, ya que la falta de esta información en el momento adecuado, puede representar pérdidas importantes para las empresas.

- **Seguridad en el Desarrollo:**

  La seguridad sobre los desarrollos que se dan dentro de la organización, esta siempre dentro de los puntos de interés de las directivas. De las ideas y proyectos que se desarrollen en las empresas dependerán su crecimiento frente a las competencia y por ningún motivo se puede permitir que se de una falla de seguridad en estas áreas que den paso a la fuga o perdida de la información relacionada.

1.2. DEFINICIÓN DE POLÍTICA DE SEGURIDAD

Las políticas de seguridad son las directrices y objetivos generales de una empresa relativos a la seguridad, expresados formalmente por la dirección general. Éstas forman parte esencial de la seguridad en las empresas y por esta razón deben ser aprobadas por la alta gerencia.

La redacción de dichas políticas varían según el gusto de cada empresa, algunas suelen ser muy extensas y complicadas; o en otras son muy cortas y breves que no se alcanza a comprender su contenido. Debido a esto es importante comprender quienes aprobaran estos documentos. En muchos casos es recomendable elaborar políticas cortas y claras que

puedan ser entendidas por todos los que leerán y estarán sujetos a éstas.

Las Políticas de Seguridad de una empresa son documentos auditables tanto para los auditores internos de la organización, como por los externos y que a su vez facilitan la obtención de nuevas certificaciones. Es de resaltar además la confianza que se consigue en los clientes quienes estarán más seguro adquiriendo productos de la empresa. Es por este motivo que las políticas de seguridad son documentos **que deben ser comprendidos más que aprendidos en todos los niveles**; desde el personal operativo/operador como por los altos mandos (directivos, gerentes, etc.).

Las empresas desean lograr a través de los documentos de políticas enfatizar su interés sobre la seguridad dentro de la organización. También que los documentos de políticas puedan ser una “Carta de presentación de la empresa” en la que se puedan identificar cuatro puntos principales. Estos puntos se pueden identificar con las siguientes preguntas: **¿A qué se dedica?, ¿qué quiere lograr?, ¿bajo qué método trabaja?, ¿Cómo lo quiere lograr?** De esta manera todos los que laboran y los que lleguen formar parte de la empresa puedan visualizar los intereses de la directiva.

1.2.1. COMPARACIÓN ENTRE POLÍTICAS, NORMAS Y LINEAMIENTOS

Las políticas son obligatorias y pueden considerarse el equivalente a una ley dentro de la organización. Se requiere de una autorización especial si algún empleado desea hacer algo que está fuera de lo contemplado en las políticas, de esta manera se asegura la empresa de que las cosas están yendo por buen camino en su establecimiento. Dado que las políticas son de carácter obligatorio, para su redacción se utilizan palabras como “no se debe hacer” o “se tiene que hacer”. Para la redacción posterior de las políticas usaremos tanto el verbo “deber” como “tener” según sea el caso.

Los lineamientos solo representan opciones y recomendaciones. En este caso, haciendo uso del verbo “deber”, una política se convertiría en un lineamiento simplemente cambiando el verbo a “debería”. Sin embargo; no se recomienda hacer esto, dado que los lineamientos violan el principio básico de diseño de sistemas seguros; es decir, que el producto tiene que ser “de aplicación universal”, y para ser un lineamiento debería ser aplicado a un grupo específico de personas.

Las normas indican requisitos técnicos específicos, frente a lo que las políticas plantean instrucciones generales. Tienen en común que tanto las normas como las políticas son de cumplimiento obligatorio. Las políticas indican lo que se debe hacer mas no detallan como deben de hacerse, mientras que las normas sí. Es por esto que se recomienda siempre que sea necesario añadir a las políticas un enunciado que indique por ejemplo que se debe proceder bajo las normas o estándares indicados. Es importante aclarar también que las políticas están diseñadas para durar un periodo de tres a cinco años y en cambio las normas varían con una mayor frecuencia.

1.2.2. COMPARACIÓN ENTRE POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

Las políticas no sólo son distintas a los procedimientos, sino que además se encuentran a un nivel mucho más superior a éstos. Los conceptos de políticas y procedimientos hay que manejarlos con mucho cuidado y por separado, ya que pueden llevar algunas veces a confusiones, perdiendo su alto índice de importancia y cumplimiento. Por ejemplo, en algunos departamentos de tecnología informática existen

procedimientos específicos para realizar los respaldos de los discos duros de los servidores. En este ejemplo, **la política** podría plantear o describir la necesidad de realizar respaldos, de tener almacenaje fuera de la sede y de salvaguardar los medios de respaldo; **el procedimiento** por su parte, podría describir que software de respaldo usar, cómo y cuándo sincronizar dichos respaldos y otros detalles.

Por otro lado tenemos al término controles, estos son también conocidos como contramedidas, medidas de seguridad y salvaguardas. **Los controles** son diferentes de las políticas, porque estos son dispositivos o mecanismos usados para guiar la operación de una máquina, aparato, sistema o un proceso.

En algunos casos, las políticas proporcionan objetivos generales y amplios que, sin los debidos controles no serían posibles su cumplimiento. Uno de estos casos puede ser cuando, "*una política que prohíba conflictos de intereses, tanto los reales como los aparentes, podría satisfacerse parcialmente a través de un control que exija a los empleados firmar una declaración donde indique que ellos han leído el código de conducta y que convienen en cumplirlo*" [1].

1.3. PROBLEMAS POR LA AUSENCIA DE POLÍTICAS DE SEGURIDAD EN LAS EMPRESAS

Como se mencionó anteriormente, a medida que la organización va creciendo, su infraestructura y su personal aumentan paralelamente. Esta situación, le exige a las empresas que tomen las medidas necesarias para salvaguardar sus bienes (imagen e integridad), que al final son los factores que le permitirán ir desarrollándose con una mayor rapidez.

El crecimiento implica el manejo de más información. Si la empresa no toma medidas para la clasificación y protección de la información, según los intereses interno y externo, corre el riesgo de que esta sea manipulada inadecuadamente o llegue a manos ajenas a la organización. Al no tener declarado y detallado, cuales son las obligaciones tanto para los empleados como para los altos ejecutivos y al no dar a conocer esto a su personal en general, la empresa podría estar enfrentando la peor situación que no solo afectaría su imagen sino también su credibilidad, esto es un problema con la justicia. Los problemas legales conllevan la mayoría de las veces al cierre definitivo de las organizaciones.

Estos son algunos de los posibles problemas que puede enfrentar una empresa si no toma la decisión de establecer políticas de seguridad. En este sentido, "*las políticas de seguridad surgen como una herramienta*

organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que favorecen al desarrollo de la organización y su buen funcionamiento" [2].

1.4. IMPORTANCIA DE LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LAS EMPRESAS

Con la gran cobertura que brindan hoy en día los medios noticiosos a la seguridad de la información, uno pensaría que los altos mandos de todas las empresas saben de qué se trata esto, lamentablemente en muchos casos no es así. Por eso, antes de empezar a redactar políticas de seguridad, hay que llevar el caso y explicarle detalladamente a la gerencia de que se trata este tema y que beneficios dará a su organización.

La importancia de la implementación de las políticas queda inmediatamente aclarada cuando analizamos problemas comunes que pueden ser resueltos o evitados con la implementación de dichas políticas. Podemos mencionar como ejemplo lo siguiente, una empresa puede adquirir una serie de productos de seguridad, pensando que estos resolverán todas sus dificultades y amenazas, pero a la hora de su implementación descubren que no alcanzan los resultados que

esperaban y todo ello debido a que no poseían un conjunto de políticas que aclararan las necesidades de la organización. Es por esto que decimos que los documentos de políticas forman parte primordial de una infraestructura de seguridad que debe tener la empresa.

Como la implementación de políticas de seguridad es un proceso técnico-administrativo, debe abarcar a toda la organización, sin exclusión alguna. Por esta razón debe tener el respaldo total de la gerencia, porque sin su ayuda, las medidas que se tomen para su implementación no tendrán la fuerza necesaria.

También es fundamental hacer conocer a todos los empleados de la organización, sobre las nuevas disposiciones que se han tomado para las mejoras de la empresa, para que haya un mejor control de las mismas.

Por todo lo expuesto anteriormente, queda claro que proponer o identificar políticas de seguridad requiere de un gran compromiso por todos los miembros de la organización, porque ayudará a minimizar fallas y debilidades y a la vez ayudará a poder renovar y actualizar dicha política en función del ambiente dinámico que se establezca y permita ir creciendo a la empresa rápidamente.

1.4.1. RESPONSABLES DE LA SEGURIDAD

Las personas encargadas de esta tarea deben ser **equilibradas y de confianza,** ya que deben ser objetivas al momento de implantar o renovar alguna política, que considere que está fallando o que no se está cumpliendo como fue deseada desde su escritura.

Por estos motivos, se debe exigir a esta persona el completo secreto confidencial y/o profesional, lo que es una garantía más de su confianza y lealtad hacia la empresa.

1.4.2. BENEFICIOS POR LA ACEPTACIÓN DE LAS POLÍTICAS

A continuación en la Tabla 1.1 se presentan los beneficios que se pueden obtener cuando la organización decide implementar las políticas de seguridad, distinguiéndose a los que beneficiarán más a: la Gerencia, al Personal y a la Empresa en su totalidad.

DIVISIONES	BENEFICIOS
GERENCIA	• El proceso de desarrollo de las políticas muestra a la gerencia lo que se requiere para incrementar la seguridad. • El proceso de desarrollo de las políticas permite establecer nuevas vías de comunicación con la alta gerencia. • Establece credibilidad y visibilidad a través del esfuerzo realizado en la seguridad. • Permite que la gerencia determine si el trabajador ejerció buen o mal juicio.
PERSONAL	• Cambia las actitudes de los trabajadores y sus perspectivas permitiendo mantener la seguridad con medidas constantes. • Permite armonizar y coordinar las actividades de muchos trabajadores lográndose calidad y eficiencia en los servicios que brinda la empresa. • Se define límites en las acciones que se pueden permitir logrando que los trabajadores entiendan los límites de sus responsabilidades asignadas. • Se evita disputas y otras querellas internas al contar con un reglamento a seguir y con límites definidos. • Se evita problemas en cuanto a la realización de tareas fuera de secuencia en asuntos cruciales, puesto que el personal no tiene la necesidad de adivinar cuales son los pasos siguientes que proceden.
EMPRESA	• Se logra controlar con anticipación los eventos relativos a la seguridad permitiendo aumentar la probabilidad de que las cosas se harán de manera correcta la primera vez y disminuyendo los errores. • Se consigue costos más bajos mediante la normalización de los controles y un mismo enfoque que se logra utilizar uniformemente a lo largo de la organización. • Establece un punto de partida de un proceso de mejoramiento continuo al representar las políticas una línea base a la cual todos pueden referirse y sobre la cual se construye el mejoramiento. • Orienta la implementación, así como la selección del servicio y del producto de seguridad. • Permite contar con documentos y obligaciones contractuales para proseguir casos en tribunales, al contar por ejemplo, con acuerdos de cumplimiento de políticas y de confidencialidad.

Tabla 1. 1 Principales beneficios que obtiene la empresa por implementar políticas de seguridad

1.4.3. FACTORES NEGATIVOS QUE SE PRODUCEN DURANTE LA IMPLEMENTACION DE LAS POLÍTICAS

La mayoría de las veces puede resultar una labor ardua y tardía, lograr convencer a la directiva, de la necesidad de implantar políticas de seguridad que ayuden al control y protección de su empresa.

Pero una vez lograda esta parte viene lo más difícil; lograr que todo el personal comprenda la importancia por la cual se han establecido estas nuevas reglas y hacerles entender que esto no va ni debe perjudicar en su trabajo; al contrario, con esto se busca mejorar y hacer más eficiente la labor de cada uno de los miembros de la empresa.

CAPÍTULO 2

DISEÑO DEL DESARROLLO DE LAS POLÍTICAS

Las políticas de seguridad son documentos que permitan a la empresa obtener un mayor grado de credibilidad y valoración hacia sus clientes; es por esto que se deben desarrollar las políticas basándose en procedimientos y definiciones estandarizadas por organismos internacionales, tales como: la norma ISO/IEC 17799:2005 y la norma ISO/IEC 27000:2009, las cuales nos ayudan con definiciones y estructuración en el documento que se elabora. Además, como en toda realización de un proyecto en el que se desea mantener un orden, con objetivos bien diferenciados y que se desea finalizar dentro de un tiempo límite, se debe contar con una guía que permita lograr dichas metas, entregando resultados

eficientes, por esto no podíamos dejar sin considerar una elaboración de pasos recomendados para un buen desarrollo y aceptación de las políticas.

2.1. HERRAMIENTAS DISPONIBLES

Entre un sin número de herramientas existentes para la elaboración de los documentos de políticas de seguridad, tenemos la norma ISO 17799, la norma ISO 27000 y la matriz de cobertura, que sin duda alguna son tres de las herramientas más fáciles de entender y comprender su uso, facilitando de igual manera la elaboración de los documentos de seguridad. Por esta razón son las herramientas utilizadas en el presente documento y que a continuación detallaremos que son y cómo las utilizaremos.

2.1.1. NORMA ISO/IEC 17799:2005

La norma ISO 17799:2005, es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

La norma ISO 17799:2005, define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. Es aquí donde se plantea, que el objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Conocer el objetivo y orientación que se le debe dar al documento de políticas de seguridad, que sugiere el estándar, es de suma importancia porque esto permitirá que el documento resalte al considerar que sigue al pie las estipulaciones que establece el estándar internacional ISO/IEC 17799:2005.

El estándar nos indica una serie de consideraciones que debemos tener tanto para la elaboración o selección de las políticas, los riesgos que se deberían analizar, como el contenido que debería tener el documento final que se presentará a la empresa.

Entre las consideraciones más importantes que se siguen en este trabajo tenemos:

- Identificación clara de los objetivos comerciales de la gerencia, obtención de su apoyo y compromiso.
- Elaboración de un documento que reciba la aprobación por parte de la gerencia y que permita ser publicado y comunicado a todos los empleados y las partes externas relevantes.
- Elaboración de políticas que justifiquen el compromiso de la gerencia y el enfoque de la organización para manejar la seguridad.
- Coordinación con los diferentes departamentos para la revisión y/o actualización de las políticas o incorporación de nuevas.
- Asignación de recursos y/o responsabilidades que se presenten debido a las políticas asignadas.

Estas consideraciones enunciadas nos encaminan hacia una correcta documentación de las políticas, logrando que obtengan el alcance deseado dentro de la empresa en que se apliquen.

El estándar también nos ofrece un listado claro de las categorías de seguridad principales que se deben analizar en toda organización. Como son:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad de Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de Comunicaciones y Operaciones.
- Control de Acceso.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de la Continuidad Comercial.
- Conformidad.

Estos temas son los que se tuvieron presentes a la hora de analizar e identificar las necesidades e intereses de seguridad, permitiendo luego decidir qué políticas o conjunto de políticas se pueden elaborar.

2.1.2. NORMA ISO/IEC 27000:2009

La norma ISO/IEC 27000:2009 forma parte de la serie 27000 publicado por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Esta provee una descripción general de los sistemas de gestión sobre la seguridad de la información. Menciona sobre las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Las organizaciones que implementen esta norma podrán obtener: una descripción general de las familias de los estándares SGSI, una introducción a la SGSI, una descripción resumida del proceso PLANIFICAR-HACER-VERIFICAR-ACTUAR (PDCA), y una aclaración de los términos y definiciones en uso a través de la familia de estándares SGSI.

El objetivo de la norma es la de proveer términos y definiciones, y una introducción a la familia de estándares SGSI, al definir los requerimientos para un estándar SGSI y la certificación de sistemas, proveer soporte directo, guías

detallada y/o interpretación para el proceso PDCA y sus requerimientos.

El proceso que elaboramos en este proyecto, está estrechamente ligado a las recomendaciones que presenta el proceso PDCA para la obtención de resultados más acertados a los requerimientos de las empresas a las cuales dirigimos este documento.

2.1.3. MATRIZ DE COBERTURA

La Matriz de Cobertura es muy útil cuando las políticas han de dirigirse a más de dos públicos, a través de documentos diferentes separados. La preparación de esta matriz, es recomendable hacerla antes de la elaboración del primer borrador de las políticas.

Una matriz de cobertura no es más que una herramienta organizacional que garantiza que todos los mensajes de seguridad de la información se presentan a las audiencias correspondientes. Es la manera en que se puede presentar el trabajo a realizar, en una manera ordenada y cubriendo las

áreas deseadas, disminuyendo gran parte del esfuerzo de redacción.

Describiendo de una manera sencilla, la matriz de cobertura es solo una tabla de dos dimensiones. Dado que seguramente habrá muchas columnas y pocas filas, se recomienda una matriz de cobertura con títulos de fila para las audiencias definidas en la empresa, los títulos de columnas en blanco para las áreas a cubrir de políticas y finalmente celdas en blanco en el medio para las políticas específicas.

En el siguiente Gráfico, se puede visualizar el modelo de la matriz de cobertura utilizada en este documento para el ordenamiento de las políticas.

	AREAS				
AUDIENCIA	**S1**	**S2**	**S3**	**S4**	**S5**
A1					
A2					
A3					

Gráfico 2. 1 Modelo de la Matriz de Cobertura

En algunas instancias, habrá semejanzas en las políticas dirigidas a las audiencias presentes. Cada vez que pueda,

haga todo lo posible para minimizar la cantidad de audiencia, pero sin descuidar que todos los grupos de la empresa obtengan la información necesaria sobre las políticas.

2.2. PASOS PARA EL PROCESO DE DESARROLLO DE POLÍTICAS

La lista que se plantea a continuación presenta en detalle, los pasos principales que se siguieron para la realización de las políticas según las recomendaciones presentadas en el manual de “Políticas de Seguridad Informática” [1], pero modificado según nuestras necesidades para el desarrollo, mejoramiento y aprobación del documento interno de la empresa.

Al final de la lista se presenta un diagrama esquemático, donde se resumen todos los pasos descritos a continuación, para lograr tener una visión general y más gráfica del proceso seguido para el desarrollo de las políticas.

Puede ser que para otra visión, algunos de los pasos siguientes se logren de manera simultánea o en orden diferente;

1) Realizar una evaluación de riesgo, para conocer las necesidades y falencias en la seguridad de la información particulares para cada

empresa. Esto fue mediante encuestas realizadas individualmente a los jefes del área encargada de la seguridad.

2) Explicar claramente que es una política dentro de la empresa, para que no confunda el concepto con los términos de procedimiento, normas o lineamientos.
3) Garantizar que la implementación de las políticas conllevará a beneficios únicos para la empresa y con ello además quedarán definidas nuevas responsabilidades que los individuos deberán cumplir.
4) Convencer al gerente que su empresa necesita políticas de seguridad documentadas, porque esto le ayudará a tener un mejor control de su organización, evitar problemas legales y conseguir un rápido crecimiento internacional.
5) Identificar los departamentos existentes en la empresa, cuáles son sus jefes o gerentes encargados, que serán quienes aprobarán el documento final de las políticas.
6) Una vez otorgado el permiso de la gerencia, recolectar y leer toda la información que contienen acerca de la seguridad interna de la empresa; ya sean políticas, normas, procedimientos o algún documento en el cual hayan detallado como tiene que ser el comportamiento u obligaciones del personal de la empresa.
7) Si la empresa no cuenta con algún documento por escrito, donde se detalle lo expuesto en el punto anterior, se procederá a realizar entrevistas acompañadas con una encuesta. Esta encuesta está

dirigida a jefes de departamento de seguridad, técnico o de IT. La elaboración de esta encuesta se detalla más adelante en este capítulo.

8) Identificar la audiencia a la cual estarán dirigidas las políticas y además tendrá gran parte de responsabilidad en el cumplimiento de cada una de ellas. Determinar si cada una tendrán un documento por separado o será publicado en una página aparte en algún sitio Intranet.
9) Verificar si esta audiencia tiene los conocimientos necesarios acerca de lo que es seguridad de la información y entiende cuán importante es y el beneficio que dará a la empresa. Nos ayudará a determinar el diseño que tendrá el documento de políticas.
10) Ya teniendo bien identificado los pasos anteriores y con la ayuda de los estatus sobre la política, así como los modelos de las políticas que se encuentran en el manual de “Políticas de Seguridad Informática” [1], procederemos a empezar a redactar el primer borrador de políticas tratando de cubrir en forma general los requerimientos de la empresa.
11) Con ayuda de la matriz de cobertura, iremos separando cada política según el área que va a proteger (identificadas con la ayuda de la evaluación de riesgo, realizada en el primer paso) y la audiencia a la cual está dirigida.
12) Presentar el primer borrador a los directivos de la empresa, mediante una reunión general con carácter de obligatorio. Identificar con ellos si

todas cubren con las necesidades y requerimientos que tiene la empresa.

13) Con los puntos establecidos en la reunión general, se redactará el documento final con las políticas específicas, que cubran todas las necesidades de la empresa.

14) Una vez aprobado por los gerentes de cada departamento y gerente general, se procederá a decidir mediante que medio se darán a conocer las políticas, lo más recomendable será por una página aparte en algún sitio Intranet de la empresa. Así todos podrán tener acceso a ella cada vez que lo requiera.

15) Llevar un seguimiento de cómo está reaccionando el personal frente a este nuevo plan de seguridad, tomando apunte de los cambios que se deberá realizar al documento en una actualización posterior.

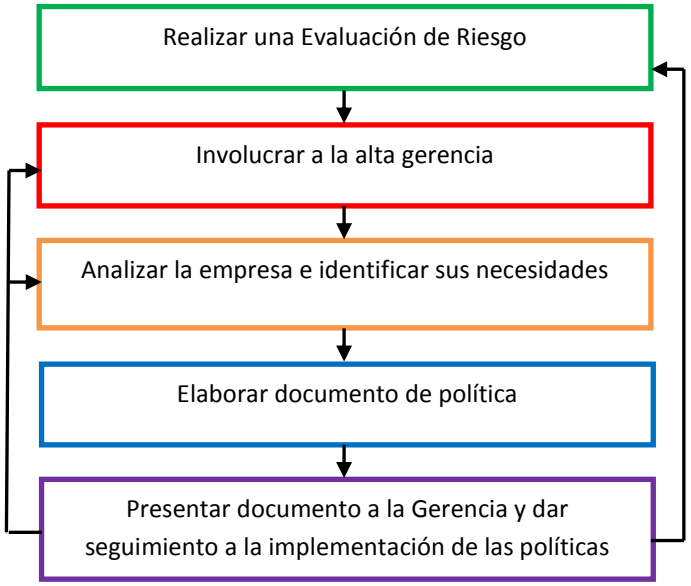


Gráfico 2. 2 Flujo para el desarrollo de las Políticas

En el Anexo D, está colocada la gráfica que detalla más ampliamente estos pasos para el proceso del desarrollo de las políticas. Tómese la molestia de revisar ya que tendrá una visualización más clara de este contenido.

2.3. CRONOGRAMA DE ACTIVIDADES PARA EL PROCESO DE DESARROLLO DE LAS POLÍTICAS

El cronograma de actividades hace parte de la estrategia operativa del proyecto de investigación. El cronograma es la descripción de las actividades en relación con el tiempo en el que se van a desarrollar. Primero hay que determinar con precisión cuáles son esas actividades a partir de los aspectos técnicos presentados en el proyecto. De acuerdo con los recursos, el tiempo total y el equipo humano con que se cuenta, se calcula para cada uno de ellos el tiempo en el cual habrán de ser desarrolladas. Para la presentación del cronograma se utilizan generalmente diagramas, los cuales permiten visualizar el tiempo de cada actividad, sobre todo en aquellos casos en que hay varias actividades en un mismo tiempo.

El cronograma que se realiza a continuación nos permitirá visualizar en tiempo cuanto nos llevara hacer la investigación y redacción de las

políticas, hasta su aceptación final. Para no entrar en detalle se mencionaran las actividades por semana de realización.

Las actividades indicadas en el siguiente cronograma, hacen referencia a los pasos mencionados en este capítulo, sección 2.2.

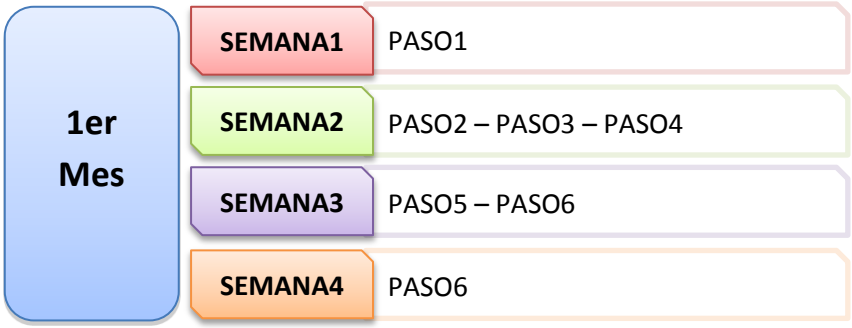


Gráfico 2. 3 Cronograma de Actividades para el primer mes

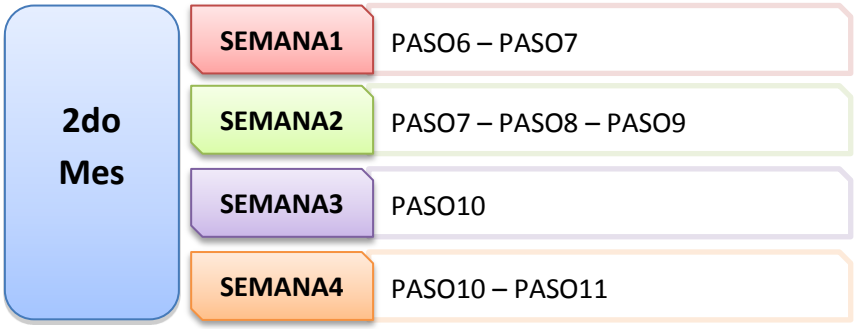


Gráfico 2. 4 Cronograma de actividades para el segundo mes

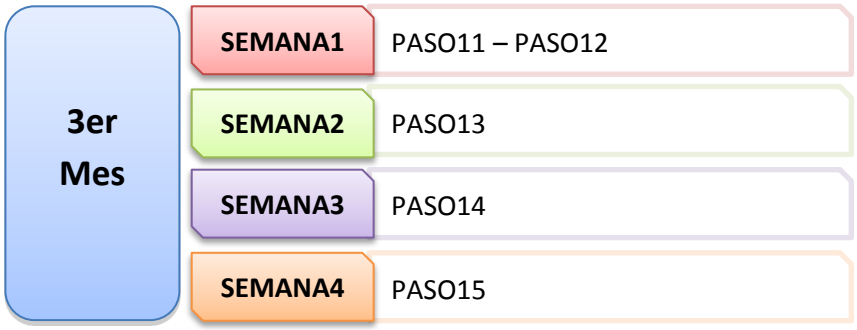


Gráfico 2. 5 Cronograma de actividades para el tercer mes

2.4. INFORMACIÓN RECAUDADA DE LA ENCUESTA A LAS EMPRESAS

La encuesta se elaboró con el fin de determinar un perfil de seguridad actual de la empresa, para luego poder seleccionar y elaborar políticas que resuelvan y mejoren el grado de seguridad.

La encuesta comprende tres partes principales: 1) Información general de la empresa, 2) Información acerca de las políticas de seguridad, e 3) Información detallada de la seguridad de la empresa.

Para un mejor entendimiento de estos puntos, daremos una breve explicación de cada uno de ellos, en el apéndice C, se encuentra el modelo de la política realizada que cumple con lo siguiente:

1) **Información general de la empresa:** La idea principal aquí, es conocer la información que maneja la empresa, que desea cuidar dentro de la misma, cuáles son sus objetivos en temas de seguridad. También deseamos identificar como está constituida su organización departamental, si posee un departamento de seguridad de la información, los diferentes cargos que se dan en cada departamento y finalmente saber cuáles son sus responsabilidades.

2) **Información acerca de las políticas de seguridad:** Con esta parte se desea saber si la empresa posee algún conjunto de políticas o si siguen políticas especificadas en alguna norma estandarizada. Identificar a la persona encargada del cumplimiento de las políticas. Saber en cuál de ellas ha tenido problemas para su cumplimiento, e identificando claramente el área problema de la empresa, para poder elaborar o mejorar un conjunto de políticas más acorde al perfil de la empresa. Conocer como ha distribuido el documento de las políticas al personal, ya que de esto depende, de que todos dentro de la empresa sepan las nuevas reglas que se manejaran. Finalmente saber cada cuanto tiempo renuevan sus políticas, ya que es recomendable que cada cinco años se modifiquen o mejoren las políticas de seguridad.

3) **Información detallada de la seguridad de la empresa:** Si la empresa posee políticas, las preguntas serán contestadas en base a ellas, caso contrario serán contestadas en base al documento donde establezcan las obligaciones y comportamiento de todos los individuos de la empresa. Con este conjunto de preguntas, se desea identificar puntos primordiales para la elaboración de las políticas, entre ellas tenemos:

- Las tecnologías y procesos que se manejan para controlar la seguridad tanto del personal y la información en la empresa.

- Saber si la información que se maneja está dividida entre secreta, confidencial, de uso interno solamente o pública.

- Determinar los controles de seguridad y que métodos tienen ya implementado para cuidar los bienes, equipos, información, áreas de trabajos, etc.

- Determinar si la empresa lleva algún control de permisos o restricciones en los diferentes departamentos.

- Saber si la empresa otorga un correo propio a los empleados, para de esa menara distinguir a su personal frente a sus distinguidos clientes.

- Saber si implementan sistemas multiusuario, los niveles de seguridad de los controles que implementan como: identificadores únicos de usuario y contraseña, clasificación de usuario en base a privilegios, firmas de declaración de conformidad, etc.

- Finalmente, conocer con qué medidas de protección cuenta la empresa para protegerse en caso de pérdidas o fugas de la información y así no se vea afectada por pérdidas de dinero perjudicando su imagen.

CAPÍTULO 3

FORMALIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD

En este capítulo se realiza la selección de las políticas de seguridad, considerando los resultados de una evaluación de riesgo. Las políticas que se presentan aquí siguen un modelo general, es decir, sobre un problema se enuncia una política con una perspectiva amplia de la solución, de tal manera que sea después fácil de modificar si se desea detallar más o dividirlas en varias políticas más específicas. También aplicaremos la elaboración de una matriz de cobertura con el objetivo de lograr un mayor ordenamiento y a su vez entendimiento del listado de política seleccionado.

3.1. EVALUACIÓN DE RIESGO

La Evaluación de Riesgo nos permite obtener una evaluación económica del impacto de los sucesos que puede ocurrir por falta de la implementación de un mecanismo de seguridad. Los valores resultantes de esta evaluación permiten contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir. La realización de este análisis nos brinda información sobre lo que las empresas desean proteger, donde y como, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se debería identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

La realización de una evaluación de riesgos enlista en prioridad, los riesgos que proporciona la información para la fase de apoyo a la toma de decisiones. El éxito de una buena evaluación de riesgo es alcanzado en cuanto más recursos y datos de interés de las empresas son determinados, clasificados y evaluados, pero este nivel de detalle, en muchas situaciones no se pueden llegar a conseguir, debido a que no siempre la empresa está dispuesta a revelar en un alto grado tal solicitud o simplemente se les dificultan y prefieren mencionar una clasificación de los recursos que cuentan y nivel de interés sobre ellos.

A continuación se presenta una lista de factores que en el caso de ocurrir, fallar, o alterarse presentaría una amenaza que perjudicaría a las empresas y sobre la cual se realiza una evaluación de riesgo basada en la opinión y nivel de interés indicado por las personas entrevistadas en las empresas y los resultados obtenidos de las encuestas realizadas.

Activos Organizativos	Amenazas de seguridad	Vulnerabilidades	Controles Actuales	Controles propuestos
- Información - Equipos - Personal	- Naturales - Intencionales - Involuntarias	- Físicas - Naturales - Por Hardware - Por Software - En Medios de Almacenamiento - En Comunicación - Humanas	- Utilización de Guardias - Controles de temperaturas - Monitoreo electrónico - Administración de cuentas de usuarios	- Servicios integrados para administración y comunicación. - Circuitos cerrados de televisión - Protección electrónica - Sistemas biométricos - Sistemas de Verificación Automática de Firmas (VAF)

Tabla 3. 1 Listado de factores de posibles riesgos de interes.

Las definiciones mencionadas en la tabla 3.2 están basadas en la recomendación que indica el Proceso de Administración de Riesgos de Seguridad de Microsoft, la cual asocia un intervalo de un año a la categoría de probabilidad alta, porque los controles de seguridad de información normalmente tardan periodos largos en implementarse.

Con la finalidad de contrastar el impacto que tendrían estos riesgos sobre las empresas mencionamos en Tabla 3.3 tres niveles de criticidad que hay que tenerlos muy en cuenta antes de iniciar la recaudación de la información.

FACTOR (ESTIMACIÓN DE PROBABILIDAD)	DEFINICIÓN	VALOR
ALTA	Muy probable, previsión de uno o varios ataques en un año.	5
MEDIA	Probable, previsión de ataques en dos a tres años.	3
BAJA	No probable, no se prevé ningún ataque en tres años.	1

Tabla 3. 2 Tabla que muestra las definiciones de los factores de probabilidad en la Evaluación de Riesgo

FACTOR (ESTIMACIÓN DE CRITICIDAD)	DEFINICIÓN	VALOR
ALTA	Muy crítico, su ocurrencia podría provocar el cierre de la empresa.	5
MEDIA	Crítico, podría provocar grandes perdidas económicas.	3
BAJA	No crítico, provocarían despidos o sanciones en el personal.	1

Tabla 3. 3 Tabla que muestra las definiciones de los factores de criticidad en la Evaluación de Riesgo

Tipos de Riesgos	Probabilidad	Criticidad	Valor
Sobre Activos de Información	ALTA	ALTA	25
Sobre Activos de Equipos	ALTA	MEDIA	15
Sobre Activos de Personal	MEDIA	BAJA	15
Amenazas Naturales	BAJA	MEDIA	15
Amenazas Intencionales	MEDIA	MEDIA	9
Amenazas Involuntarias	BAJA	BAJA	1
Vulnerabilidades Físicas	BAJA	MEDIA	3
Vulnerabilidades Naturales	BAJA	MEDIA	3
Vulnerabilidades por Hardware	MEDIA	MEDIA	9
Vulnerabilidades por Software	MEDIA	MEDIA	9
Vulnerabilidades en Medios de Almacenamiento	ALTA	BAJA	5
Vulnerabilidades en Comunicación	ALTA	MEDIA	15
Vulnerabilidades Humanas	MEDIA	BAJA	3
Utilización de Guardias	BAJA	BAJA	1
Controles de temperaturas	MEDIA	MEDIA	9
Monitoreo electrónico	MEDIA	BAJA	3
Administración de cuentas de usuarios	ALTA	BAJA	5
Servicios integrados para administración y comunicación	MEDIA	MEDIA	9
Circuitos cerrados de televisión	BAJA	BAJA	1
Protección electrónica	MEDIA	MEDIA	9
Sistemas biométricos	MEDIA	MEDIA	9
Sistemas de Verificación Automática de Firmas (VAF)	BAJA	MEDIA	3

Tabla 3. 4 Se muestra los diferentes Tipos de Riesgos, junto con su factor de probabilidad según la Tabla 3.1

Se observa en la tabla 3.4, que para las empresas las amenazas que involucran: la información, los equipos, el estado de los medios de almacenamiento, los procesos de comunicación en general y la administración sobre los usuarios, es en temas de seguridad una necesidad que se debe resolver con mayor prioridad. En el anexo F

presentamos una tabla resumen de la evaluación que permite apreciar de una mejor manera los resultados. Determinamos que los riesgos con una mayor valoración afectarían a la empresa con severidad en caso de presentarse. Las demás amenazas expuestas se observa que son consideradas con una menor prioridad y reservándonos por un momento las opiniones de cuales deberían incrementar de nivel, se debe recordar que lo que se busca es la aceptación de la implementación de las políticas de seguridad como alternativa de solución para las necesidades inmediatas de la empresa. Con esto en claro se procede en los próximos temas, a la selección de políticas que en primera instancia cubran de manera general todas las necesidades, teniendo presente siempre las prioridades resultantes de la evaluación de riesgo. Y posteriormente a las propuestas de implementación sugeridas que contemplarán las amenazas con mayores niveles de ocurrencia para las empresas.

3.2. LISTADO GENERAL DE POLÍTICAS

La selección de las políticas deben cubrir de manera general todos los problemas que las empresas poseen y podrían llegar a presentarse en algún momento. Al mismo tiempo hay que cuidarse de no diseñar un documento de política demasiado extenso la primera vez que se elabora, se debe intentar abarcar lo primordial y luego cuando se haya logrado esto y el documento haya sido aprobado por la gerencia, se puede

trabajar sobre este y con el transcurso del tiempo, se irán anotado las observaciones que se vayan presentando y cuando llegue el momento de su actualización se cubran con estos y otros puntos para mejoras del documento de políticas de la empresa.

Haciendo uso de las políticas de alto nivel propuestas en el manual de “Políticas de Seguridad Informática” [1], se hará un listado general de políticas que más se acomoden al perfil de las empresas entrevistadas e ir cubriendo de esta manera sus requerimientos y necesidades. La ventaja que presenta la selección de políticas que siguen un modelo general es que en caso de requerir cambios, estas se prestan para ser modificadas en políticas más específicas si se lo requiere.

A continuación, se enlistan por título cada política y según el orden en que aparecen en el manual de “Políticas de Seguridad Informática” [1]. En el Anexo A se encuentran la lista de todas estas políticas y sus características.

1. *Rol de la Información y los Sistemas informáticos.*
2. *Esfuerzo de Equipo.*
3. *Personas Involucradas.*
4. *Propiedad de Archivos y Mensajes.*
5. *Principales Departamentos que Trabajan en Seguridad de la Información.*
6. *Tres Categorías de Responsabilidad.*
7. *Responsabilidades del Propietario.*
8. *Responsabilidades del Custodio.*
9. *Responsabilidades del Usuario.*
10. *Manejo Consistente de la Información.*

11. *Designaciones para la Clasificación de la Información.*
12. *Etiquetado de la Clasificación de la Información.*
13. *Necesidad de Conocer.*
14. *Identificadores de Usuario y Contraseñas.*
15. *Identificadores de Usuarios Anónimos.*
16. *Contraseñas Difíciles de Adivinar.*
17. *Contraseñas Fáciles de Recordar.*
18. *Patrones Repetitivos en Contraseñas.*
19. *Restricciones de las Contraseñas.*
20. *Almacenamiento de las Contraseñas.*
21. *Compartir Contraseñas.*
22. *Declaración de Conformidad.*
23. *Divulgación de Información a Terceros.*
24. *Solicitud de Terceros de Información de la empresa.*
25. *Seguridad Física para Controlar el Acceso a la Información.*
26. *Conexiones Internas de Red.*
27. *Conexiones Externas de Red.*
28. Modificaciones a las Redes.
29. *Teletrabajo.*
30. *Acceso a Internet.*
31. *Correo Electrónico.*
32. *Software antivirus.*
33. *Erradicación de Virus.*
34. *Respaldos Limpios.*
35. *Fuentes de Software.*
36. *Especificaciones Escritas para los Propietarios.*
37. *Requisito de Autorización por Seguridad.*
38. *Control Formal de Cambios.*
39. *Convenciones para Desarrollo de Sistemas.*
40. *Licencias Adecuadas.*
41. *Copias No Autorizadas.*
42. *Responsabilidad de Respaldar.*
43. *Protección Antirrobo.*
44. *Divulgación de la Información de Seguridad.*
45. *Derechos sobre el Material Desarrollado.*
46. *Derecho a Investigar y Monitorear.*
47. *Uso Personal.*
48. *Conducta Inapropiada.*
49. *Herramientas que Comprometen la Seguridad.*
50. *Actividades Prohibidas.*
51. *Informes Obligatorios.*
52. *Plan de Seguridad Física.*

53. *Ubicación del Centro de Computación y Comunicaciones.*
54. *Distintivos de Identificación.*
55. *Distintivos Personales.*
56. *Entradas Individuales.*
57. *Documentación de las Aplicaciones de Producción.*
58. *Implementación de Sistemas Multiusuario.*
59. *Análisis del Impacto sobre la Seguridad Informática.*
60. *Comité de Gestión de Seguridad Informática.*

Más adelante, en este capítulo y con la ayuda de la matriz de cobertura se presentarán estas mismas políticas pero ordenadas según las audiencias establecidas. Así, se tendrá una mejor visualización de que política le corresponde a cada grupo del personal y que área debe cubrir bajo estos conceptos.

3.3. ELABORACIÓN DE MATRIZ DE COBERTURA

Como ya se mencionó en el capítulo anterior, la matriz de cobertura no es más que una herramienta que nos permitirá ordenar las políticas según unas áreas y audiencias establecidas previamente. Haciendo uso de la matriz, lograremos ordenar el listado de políticas anteriormente mencionadas en este capítulo, una vez conseguido este propósito podemos dirigir de mejor manera el conjunto de políticas a una audiencia final.

3.3.1. DEFINICIÓN DE AUDIENCIAS

La asignación de las audiencias es un proceso muy importante, porque serán las personas a la cuales van a estar dirigidas las políticas y a quienes se les asignará los permisos y negaciones para hacer uso de los bienes e información de la empresa.

Luego de las observaciones realizadas en cada empresa visitada, se identificó la coincidencia de tres grupos de personal que las conformaban; por esta razón, se decidió elegir el siguiente grupo de audiencias que cumplan con lo existente en las empresas. De esta manera la orientación de las políticas se las puede elaborar sin dar preferencia a una empresa en particular.

En la tabla 3.5, se mencionan las audiencias establecidas junto con sus respectivas definiciones, a las cuales son dirigidas la elaboración del documento de políticas.

AUDIENCIAS	DEFINICIÓN
Gerencia	Audiencia encargada de tomar las decisiones en la empresa. (Encargadas de aprobar las políticas).
Departamento Técnico o de IT	Audiencia encargada de administrar, instalar y cuidar los sistemas dentro de la empresa.
Usuarios Finales	Audiencia que hacen usos de los servicios y activos de la empresa.

Tabla 3. 5 Lista de Audiencias y sus definiciones

3.3.2. DEFINICIÓN DE ÁREAS

La definición de las áreas es un proceso primordial para la elaboración del documento de políticas, una correcta definición del área logra que la implementación de las políticas sea más certera al permitir a las audiencias a quienes se les dirige las políticas, entender el objetivo y el alcance que se desea conseguir con las mismas. También es fundamental para lograr un orden en los documentos que deriven del manual de políticas.

Con la finalidad de cubrir en gran parte todas las necesidades que tienen las empresas en común, identificamos cinco áreas (Tabla 3.6), que se presentan de manera similar en cada una de ellas.

ÁREAS	DEFINICIÓN
Ordenadores	Área que relaciona todos los computadores personales de la empresa.
Seguridad Física	Todo lo que concierne al ambiente donde se ubican los equipos y se labora.
Comunicación y Manejo de Datos	Todo lo que concierne a los procesos de comunicación, administración de la información, etc.
Gestión de Riesgo	Se contempla todo lo relacionado a las medidas y contramedidas que se presenten o se llegaran a presentar por causas físicas o legales.
Equipos de Comunicación de Datos	Todo lo referente a equipos que forman parte de la red de comunicación de datos de la empresa.

Tabla 3. 6 Lista de las Áreas junto con sus definiciones

3.3.3. PLANTEAMIENTO DE LA MATRIZ DE COBERTURA

Una vez definidas las audiencias y áreas a las cuales serán orientadas el documento de las políticas, se procede a armar la matriz de cobertura como paso esencial para la presentación final y general de las políticas.

La matriz es diseñada colocando en la primera columna todas las audiencias y en la primera fila las áreas. Las celdas restantes servirán para ir colocando las políticas que se acomoden a la audiencia y área que representan. Ordenando éstas, según su número establecido en el Listado General de Políticas, para que los usuarios puedan guiarse mejor a través del documento de políticas.

En la tabla 3.7, se presenta el diseño general de la matriz de cobertura, donde se ha colocado ya las políticas divididas y que cubran la seguridad de cada área establecida.

	AREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FISICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTION DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
GERENCIA	N.A.	25-52-53	1-4-11-23-24-45-59-60	3-5-6-7-8-9-28-29-40-46-48	N.A.
DEPARTAMENTO TECNICO	15-16-17-18-19-20-21-27-32-33-35-38-39	14-25-26-43-53-56	1-10-11-13-23-42-47-57-58-59	2-3-5-6-7-8-9-28-29-30-31-34-36-37-41-44-46-48-49	15-16-17-18-19-20-21-22-27-35-38-39
USUARIOS FINALES	15-16-17-18-19-20-21-32-33	25-43-54-55	1-4-11-12-13-23-24-42-45-47-58	2-3-9-28-29-30-31-37-41-46-48-49-50-51	N.A.

Tabla 3. 7 Matriz de Cobertura con todas las políticas divididas según el área y audiencia requerida

Ahora, con la matriz de cobertura formada se puede elaborar un índice del listado de las políticas diferente para cada audiencia y ordenado por las áreas, logrando así que el público objetivo pueda concentrarse más en las políticas que les conciernen.

3.4. PRESENTACIÓN ORDENADA DE LAS POLÍTICAS

Una estrategia para la aceptación de las políticas de seguridad por parte del personal de la empresa, es que los mismos no se sientan estresados por el amplio conjunto de reglas que la empresa ha decidido aplicar para la mejora de su seguridad. Esto se puede lograr, creando un documento ordenado y que las personas puedan seguir y encontrar en él fácilmente las nuevas políticas a las cuáles se regirán de ahora en adelante.

Índice para la Gerencia

Un documento para la gerencia requiere que en él se resalte información que tiene como fin inmediato la integridad de la empresa y donde la gerencia tenga una participación activa para lograr su formalización.

Con el listado de políticas, diseñamos el índice propuesto para la gerencia (Tabla 3.9). Como se puede observar, no se cuentan con políticas en el área de ordenadores ni en Equipos de Comunicación de Datos, debido a que las políticas en estas áreas no requieren de la participación de la gerencia para aplicar dichas políticas. En cambio, se seleccionaron políticas orientadas al manejo de la información y políticas que provocarán cambios en los procesos internos o externos y de reasignación de funciones.

	ÁREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FISICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTION DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
GERENCIA	N.A.	25-52-53	1-4-11-23-24-45-59-60	3-5-6-7-8-9-28-29-40-46-48	N.A.

Tabla 3. 8 Matriz de Cobertura para la Audiencia "Gerencia".

AUDIENCIA	ÍNDICE
GERENCIA	**SEGURIDAD FÍSICA:** - Seguridad Física para Controlar el Acceso a la Información. (25) - Plan de Seguridad Física (52) - Ubicación del Centro de Computación y Comunicaciones (53) **COMUNICACIÓN Y MANEJO DE DATOS:** - Rol de la Información y los Sistemas informáticos. (1) - Propiedad de Archivos y Mensajes. (4) - Designaciones para la Clasificación de la Información. (11) - Divulgación de Información a Terceros. (23) - Solicitud de Terceros de Información de la empresa. (24) - Derechos sobre el Material Desarrollado. (45) - Análisis del Impacto sobre la Seguridad Informática (59) - Comité de Gestión de Seguridad Informática (60) **GESTIÓN DE RIESGO:** - Personas Involucradas. (3) - Principales Departamentos que Trabajan en Seguridad de la Información. (5) - Tres Categorías de Responsabilidad. (6) - Responsabilidades del Propietario. (7) - Responsabilidades del Custodio. (8) - Responsabilidades del Usuario. (9) - Modificaciones a las Redes. (28) - Teletrabajo. (29) - Licencias Adecuadas. (40) - Derecho a Investigar y Monitorear. (46) - Conducta Inapropiada. (48)

Tabla 3. 9 Índice General de Políticas para la Gerencia.

Índice para el Departamento Técnico

En la tabla 3.10, se muestra las divisiones para las áreas donde el departamento técnico será el encargado de cumplir las políticas asignadas. Y con esta distribución generamos el índice general que se presenta en la tabla 3.11. Estas políticas tienen la cualidad de que provocan cambios o actualizaciones en el hardware y software, y solo el departamento técnico tiene la obligación de adaptarlas a la organización para cumplir con las nuevas medidas que las políticas traerán. También se puede notar, que a diferencia de las otras audiencias, esta cuenta con mayor número de políticas lo cual se debe al hecho de que las empresas a las cuales están dirigidos los documentos de políticas, siguen un perfil de empresas tecnológicas que cuentan con sistemas integrados de Hardware y Software en una mayor proporción.

	ÁREAS				
AUDIENCIA	**ORDENADORES**	**SEGURIDAD FISICA**	**COMUNICACIÓN Y MANEJO DE DATOS**	**GESTIÓN DE RIESGO**	**EQUIPOS DE COMUNICACIÓN DE DATOS**
DEPARTAMENTO TÉCNICO	15-16-17-18-19-20-21-27-32-33-35-38-39	14-25-26-43-53-56	1-10-11-13-23-42-47-57-58-59	2-3-5-6-7-8-9-28-29-30-31-34-36-37-41-44-46-48-49	15-16-17-18-19-20-21-22-27-35-38-39

Tabla 3. 10 Matriz de Cobertura para la Audiencia "Departamento Técnico".

AUDIENCIA	ÍNDICE
DPTO. TÉCNICO	**ORDENADORES:** - Identificadores de Usuarios Anónimos. (15) - Contraseñas Difíciles de Adivinar. (16) - Contraseñas Fáciles de Recordar. (17) - Patrones Repetitivos en Contraseñas. (18) - Restricciones de las Contraseñas. (19) - Almacenamiento de las Contraseñas. (20) - Compartir Contraseñas. (21) - Conexiones Externas de Red. (27) - Software antivirus. (32) - Erradicación de Virus. (33) - Fuentes de Software. (35) - Control Formal de Cambios. (38) - Convenciones para Desarrollo de Sistemas. (39) **SEGURIDAD FÍSICA:** - Identificadores de Usuario y Contraseñas. (14) - Seguridad Física para Controlar el Acceso a la Información. (25) - Conexiones Internas de Red. (26) - Protección Antirrobo. (43) - Ubicación del Centro de Computación y Comunicaciones (53) - Entradas Individuales (56) **COMUNICACIÓN Y MANEJO DE DATOS:** - Rol de la Información y los Sistemas informáticos. (1) - Manejo Consistente de la Información. (10) - Designaciones para la Clasificación de la Información. (11) - Necesidad de Conocer. (13) - Divulgación de Información a Terceros. (23) - Responsabilidad de Respaldar. (42) - Uso Personal. (47) - Documentación de las Aplicaciones de Producción (57) - Implantación de Sistemas Multiusuario (58) - Análisis del Impacto sobre la Seguridad Informática (59) **EQUIPOS DE COMUNICACIÓN DE DATOS:** - Identificadores de Usuarios Anónimos. (15) - Contraseñas Difíciles de Adivinar. (16) - Contraseñas Fáciles de Recordar. (17) - Patrones Repetitivos en Contraseñas. (18) - Restricciones de las Contraseñas. (19) - Almacenamiento de las Contraseñas. (20) - Compartir Contraseñas. (21) - Declaración de Conformidad. (22) - Conexiones Externas de Red. (27) - Fuentes de Software. (35) - Control Formal de Cambios. (38) - Convenciones para Desarrollo de Sistemas. (39)

Tabla 3. 11 Índice General de Políticas para el Departamento Técnico

AUDIENCIA	ÍNDICE
DPTO. TÉCNICO	**GESTIÓN DE RIESGO:** - Esfuerzo de Equipo. (2) - Personas Involucradas. (3) - Principales Departamentos que Trabajan en Seguridad de la Información. (5) - Tres Categorías de Responsabilidad. (6) - Responsabilidades del Propietario. (7) - Responsabilidades del Custodio. (8) - Responsabilidades del Usuario. (9) - Modificaciones a las Redes. (28) - Teletrabajo. (29) - Acceso a Internet. (30) - Correo Electrónico. (31) - Respaldos Limpios. (34) - Especificaciones Escritas para los Propietarios. (36) - Requisito de Autorización por Seguridad. (37) - Copias No Autorizadas. (41) - Divulgación de la Información de Seguridad. (44) - Derecho a Investigar y Monitorear. (46) - Conducta Inapropiada. (48) - Herramientas que Comprometen la Seguridad. (49)

Tabla 3. 12 Índice General de Políticas para el Departamento Técnico (Continuación)

Índice para los Usuarios Finales

La tabla 3.12 presenta como será la distribución de las políticas para los usuarios finales, con las que luego formaremos el índice general para esta audiencia (Tabla 3.13). Las asignaciones de estas políticas tienen como fin indicar a los usuarios finales de la organización como debe ser el proceder con la información y el manejo de sus activos y al mismo tiempo incrementar la seguridad. También notamos que no se plantea políticas sobre el área de Equipos de Comunicación de Datos, debido a que los usuarios finales comunes no son los encargados de manejar este segmento de la organización ya que para esto se cuenta con personal asignado del Departamento Técnico.

	ÁREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FÍSICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTIÓN DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
USUARIOS FINALES	15-16-17-18-19-20-21-32-33	25-43-54-55	1-4-11-12-13-23-24-42-45-47-58	2-3-9-28-29-30-31-37-41-46-48-49-50-51	N.A.

Tabla 3. 13 Matriz de cobertura para la audiencia "Usuarios Finales".

AUDIENCIA	ÍNDICE
USUARIOS FINALES	**ORDENADORES:** - Identificadores de Usuarios Anónimos. (15) - Contraseñas Difíciles de Adivinar. (16) - Contraseñas Fáciles de Recordar. (17) - Patrones Repetitivos en Contraseñas. (18) - Restricciones de las Contraseñas. (19) - Almacenamiento de las Contraseñas. (20) - Compartir Contraseñas. (21) - Software antivirus. (32) - Erradicación de Virus. (33) **SEGURIDAD FÍSICA:** - Seguridad Física para Controlar el Acceso a la Información. (25) - Protección Antirrobo. (43) - Distintivos de Identificación (54) - Distintivos Temporales (55) **COMUNICACIÓN Y MANEJO DE DATOS:** - Rol de la Información y los Sistemas informáticos. (1) - Propiedad de Archivos y Mensajes. (4) - Designaciones para la Clasificación de la Información. (11) - Etiquetado de la Clasificación de la Información. (12) - Necesidad de Conocer. (13) - Divulgación de Información a Terceros.(23) - Solicitud de Terceros de Información de la empresa. (24) - Responsabilidad de Respaldar. (42) - Derechos sobre el Material Desarrollado. (45) - Uso Personal. (47) - Implantación de Sistemas Multiusuario (58) **GESTIÓN DE RIESGO:** - Esfuerzo de Equipo. (2) - Personas Involucradas. (3) - Responsabilidades del Usuario.(9) - Modificaciones a las Redes. (28) - Teletrabajo. (29) - Acceso a Internet. (30) - Correo Electrónico. (31) - Requisito de Autorización por Seguridad. (37) - Copias No Autorizadas. (41) - Derecho a Investigar y Monitorear. (46) - Conducta Inapropiada. (48) - Herramientas que Comprometen la Seguridad. (49) - Actividades Prohibidas. (50) - Informes Obligatorios. (51)

Tabla 3. 14 Índice General de Políticas para los Usuarios Finales.

CAPÍTULO 4

APROBACIÓN Y DISEÑO DE PROCESO DE MEJORAMIENTO CONTINUO DE LAS POLÍTICAS

En este capítulo detallamos los documentos finales para cada audiencia, según las políticas iniciales que se tengan que implementar para que la empresa ya haga uso del manual de políticas. Esto lo haremos presentando una matriz de cobertura separada que resaltará las políticas de mayor interés o prioridad para la audiencia a la que se le dirige. Como ya se habló anteriormente, no basta implementar algo y pensar que esto funcionará por siempre, es necesario, por no decir obligatorio, seguir un proceso de seguimiento del documento de políticas implementado, que permita mantener siempre las políticas acorde con el crecimiento de la empresa. Y es por esto, que aquí se presenta unos breves pasos que resuman como debería realizarse de manera efectiva este seguimiento.

4.1. IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Para lograr una aceptación de las políticas por parte de las audiencias involucradas, se les debe exponer primero un grupo de políticas resumidas, las cuales representen en un corto plazo cambios positivos dentro de la organización. Deben estas políticas seleccionadas ser un reflejo directo de una gran decisión tomada por la gerencia y que al ser apoyadas por los que conforman la empresa, den paso a una implementación total de las políticas elaboradas en este documento.

Teniendo este objetivo primordial claro, a continuación se presenta en una matriz de cobertura el índice de las políticas que se consideran de mayor interés, permitiendo reflejar una mejora significativa de la seguridad al ser aplicadas en la empresa.

	ÁREAS				
AUDIENCIA	**ORDENADORES**	**SEGURIDAD FÍSICA**	**COMUNICACIÓN Y MANEJO DE DATOS**	**GESTIÓN DE RIESGO**	**EQUIPOS DE COMUNICACIÓN DE DATOS**
GERENCIA	**N.A.**	**25-52-53**	**1-4-11-23-24-45-59-60**	**3-5a-5-6-7-8-9-28-29-40-46-48**	**N.A.**
DEPARTAMENTO TÉCNICO	**15-16-17-18-19-20-21-27-32a-32-33-35-38-39**	**14-25-26-43-53-56**	**1-10-11-13-23-42-47-57-58-59**	**2-3-5a-5-6-7-8-9-28-29-30-31-34-36-37-41-44-46-48-49**	**15-16-17-18-19-20-21-22-27-35-38-39**
USUARIOS FINALES	**15-16-17-18-19-20-21-32a-32-33**	**25-43-54-55**	**1-4-11-12-13-23-24-42-45-47-58**	**2-3-9-28-29-30-31-37-41-46-48-49-50-51**	**N.A.**

Tabla 4. 1 Matriz de Cobertura resaltando las políticas a implementares inmediatamente.

Con las políticas de interés ya seleccionadas de color rojo, procedemos a continuación a presentar el índice resultante con las políticas que se implementaran inicialmente.

Índice de Políticas Iniciales para la Gerencia

Las políticas seleccionadas en la Tabla 4.2, y que presentamos en forma de índice el la siguiente Tabla 4.3, son políticas de interés para la Gerencia y orientadas para empresas pequeñas o medianas, que desean comenzar a incrementar su seguridad sin llegar a una gran inversión inicialmente, estas políticas en su mayoría pueden conseguir su objetivo con personal y equipos que ya se cuentan en las empresas.

	ÁREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FÍSICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTIÓN DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
GERENCIA (INICIAL)	N.A.	25	1-4-11-23-24-45	3-5a-6-7-8-9-28-46-48	N.A.
GERENCIA (FINAL)	N.A.	52-53	59-60	5-29-40	N.A.

Tabla 4. 2 Matriz de Cobertura con las políticas iniciales para la Gerencia.

AUDIENCIA	ÍNDICE
GERENCIA	**SEGURIDAD FÍSICA:** - Seguridad Física para Controlar el Acceso a la Información. (25) **COMUNICACIÓN Y MANEJO DE DATOS:** - Rol de la Información y los Sistemas informáticos. (1) - Propiedad de Archivos y Mensajes. (4) - Designaciones para la Clasificación de la Información. (11) - Divulgación de Información a Terceros. (23) - Solicitud de Terceros de Información de la empresa. (24) - Derechos sobre el Material Desarrollado. (45) **GESTIÓN DE RIESGO:** - Personas Involucradas. (3) - Principales Departamentos que Trabajan en Seguridad de la Información. (5a) - Tres Categorías de Responsabilidad. (6) - Responsabilidades del Propietario. (7) - Responsabilidades del Custodio. (8) - Responsabilidades del Usuario. (9) - Modificaciones a las Redes. (28) - Derecho a Investigar y Monitorear. (46) - Conducta Inapropiada. (48)

Tabla 4. 3 Índice inicial de las Políticas para la Gerencia

Índice de Políticas Iniciales para el Departamento Técnico

Similar a la matriz de la Tabla 4.2, se hizo la selección de las políticas en base a las necesidades inmediatas que tienen las empresas pequeñas o medianas, garantizando un incremento en su seguridad pero ocupando los recursos existentes en la empresa. De igual manera en la Tabla 4.5, tenemos el índice con los títulos de las políticas a implementarse para el Departamento Técnico según las áreas establecidas.

	ÁREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FÍSICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTIÓN DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
DPTO. TÉCNICO (INICIAL)	15-19-20-27-32a-33-35-38	14-25-26-43	1-10-11-13-42-47	3-5a-6-7-8-9-28-30-31-34-37-41-46-48	15-19-20-22-35-38
DPTO. TÉCNICO (FINAL)	16-17-18-21-32-39	53-56	23-57-58-59	2-5-29-36-44-49	16-17-18-21-27-39

Tabla 4. 4 Matriz de Cobertura con las políticas iniciales para el Departamento Técnico.

AUDIENCIA	ÍNDICE
DPTO. TÉCNICO	**ORDENADORES:** - Identificadores de Usuarios Anónimos. (15) - Restricciones de las Contraseñas. (19) - Almacenamiento de las Contraseñas. (20) - Conexiones Externas de Red. (27) - Software antivirus. (32a) - Erradicación de Virus. (33) - Fuentes de Software. (35) - Control Formal de Cambios. (38) **SEGURIDAD FÍSICA:** - Identificadores de Usuario y Contraseñas. (14) - Seguridad Física para Controlar el Acceso a la Información. (25) - Conexiones Internas de Red. (26) - Protección Antirrobo. (43) **COMUNICACIÓN Y MANEJO DE DATOS:** - Rol de la Información y los Sistemas informáticos. (1) - Manejo Consistente de la Información. (10) - Designaciones para la Clasificación de la Información. (11) - Necesidad de Conocer. (13) - Responsabilidad de Respaldar. (42) - Uso Personal. (47) **GESTIÓN DE RIESGO:** - Personas Involucradas. (3) - Principales Departamentos que Trabajan en Seguridad de la Información. (5a) - Tres Categorías de Responsabilidad. (6) - Responsabilidades del Propietario. (7) - Responsabilidades del Custodio. (8) - Responsabilidades del Usuario. (9) - Modificaciones a las Redes. (28) - Acceso a Internet. (30) - Correo Electrónico. (31) - Respaldos Limpios. (34) - Requisito de Autorización por Seguridad. (37) - Copias No Autorizadas. (41) - Derecho a Investigar y Monitorear. (46) - Conducta Inapropiada. (48) **EQUIPOS DE COMUNICACIÓN DE DATOS:** - Identificadores de Usuarios Anónimos. (15) - Restricciones de las Contraseñas. (19) - Almacenamiento de las Contraseñas. (20) - Declaración de Conformidad. (22) - Fuentes de Software. (35) - Control Formal de Cambios. (38)

Tabla 4. 5 Índice inicial de las Políticas para el Departamento Técnico.

Índice de Políticas Iniciales para los Usuarios Finales

En la Tabla 4.6, se observan las políticas más relevantes para uso de los Usuarios Finales y que ayuda a la empresa a incrementar la seguridad con la misma idea que las políticas anteriores, es decir ocupando los recursos existentes en la organización y con el tiempo se podrán ir mejorando según las necesidades y requerimientos que las empresas establezcan.

Recuerde que ya teniendo la aprobación de la gerencia general y finalmente con estos índices establecidos se procede a separar los documentos según la audiencia a la cual están dirigidas, para que puedan ser distribuidas más fácilmente y por ende rápidamente entendidas.

	ÁREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FÍSICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTIÓN DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
USUARIOS FINALES (INICIAL)	15-19-20-32a-33	25-54	1-4-12-13-23-24-42-45	3-9-28-30-31-37-41-46-48-50-51	N.A.
USUARIOS FINALES (FINAL)	16-17-18-21-32	43-55	11-47-58	2-29-49	N.A.

Tabla 4. 6 Matriz de Cobertura con las políticas iniciales para el Departamento Técnico.

AUDIENCIA	ÍNDICE
USUARIOS FINALES	**ORDENADORES:** - Identificadores de Usuarios Anónimos. (15) - Restricciones de las Contraseñas. (19) - Almacenamiento de las Contraseñas. (20) - Software antivirus. (32a) - Erradicación de Virus. (33) **SEGURIDAD FÍSICA:** - Seguridad Física para Controlar el Acceso a la Información. (25) - Distintivos de Identificación (54) **COMUNICACIÓN Y MANEJO DE DATOS:** - Rol de la Información y los Sistemas informáticos. (1) - Propiedad de Archivos y Mensajes. (4) - Etiquetado de la Clasificación de la Información. (12) - Necesidad de Conocer. (13) - Divulgación de Información a Terceros.(23) - Solicitud de Terceros de Información de la empresa. (24) - Responsabilidad de Respaldar. (42) - Derechos sobre el Material Desarrollado. (45) **GESTIÓN DE RIESGO:** - Personas Involucradas. (3) - Responsabilidades del Usuario.(9) - Modificaciones a las Redes. (28) - Acceso a Internet. (30) - Correo Electrónico. (31) - Requisito de Autorización por Seguridad. (37) - Copias No Autorizadas. (41) - Derecho a Investigar y Monitorear. (46) - Conducta Inapropiada. (48) - Actividades Prohibidas. (50) - Informes Obligatorios. (51)

Tabla 4. 7 Índice inicial de las Políticas para el Departamento Técnico.

Es recomendable inicialmente tener una reunión general con los jefes o gerentes de cada departamento para que ellos las entiendan y se comprometan a hacerlas cumplir con el grado de obligación, y luego se procederá a reunirse con el personal de toda la organización para que sepan las nuevas medidas y cambios que se han tomado y que será deber de todos cumplirlas para lograr el bienestar y éxito de la empresa.

4.2. SEGUIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

Los procesos de mejoramiento continuo recomiendan que después de toda implementación se realice un seguimiento que evalué y recopile todos los cambios que se produzcan. La mejora continua del proyecto va ligada estrechamente al incremento de la seguridad dentro de la organización.

Cuesta considerar que la puesta en marcha del documento de políticas dentro de la empresa se adapte plenamente, siempre habrá factores que tal vez desde que se comenzó a elaborarse el documento de políticas surgieron y deberá ahora ser considerado para una actualización próxima. Estos factores podrían ser, la implementación de un nuevo departamento con ciertas funcionalidades y recursos no cubiertos adecuadamente por las políticas existentes, ciertas amenazas que se dieron y ofrecieron nuevos puntos de vistas que deberían ser atendidos con mayor prioridad, surgiendo la necesidad de escribir políticas más específicas sobre el tema, y otro factor que se podría dar es un rechazo de ciertas medidas producto de las políticas. Estos hechos son razones que si no se les da un correcto análisis la gerencia podría empezar a ver con cierta negatividad la idea de las políticas y lo que en un principio se deseaba, crear un ambiente laboral seguro y cómodo, podría empezar a resultar en lo opuesto.

La solución para esto puede llegar a ser simple si se sigue un programa de seguimiento que recolecte de manera ordenada y detallada todas las

irregularidades después de la implementación, siendo ejemplo para todos los que integran la empresa, que lo que se desea es obtener un documento de políticas facilitador de las labores diarias con altos grados de seguridad y no la realización de un proyecto que termine siendo un fracaso.

Puesto en claro la importancia que posee el hecho de seguir un programa de mejoramiento de las políticas, a continuación se enlista una serie de pasos que se pueden seguir para lograr mejores resultados del documento de políticas de seguridad.

Pasos para la mejora continua de las políticas

1. Se debe colocar el documento al alcance de todos los usuarios y asegurándose además que se pueda desplazar cómodamente a través de este. Se podría lograr esto colocándolo en un sitio web para uso interno de la empresa, con enlaces hacia las políticas, uso de motores de búsqueda de palabras claves. Debe estar elaborado de tal manera que los usuarios solo se concentren en las políticas de interés para ellos.

2. Se debe ofrecer la oportunidad que los usuarios opinen sobre las políticas, es importante conocer desde el punto de vista del usuario su impresión de las políticas. Los usuarios podrían incluso

mediante sus opiniones identificar ciertos requerimientos que las políticas no cubren, y que consideran que deberían. Esto se puede conseguir mediante la elaboración de cuestionarios que se los pueden hacer llegar en pequeños bancos de preguntas que no les tomen más de un minuto o dos cooperar, también este mecanismo puede permitir que el personal se integre con las políticas.

3. La elaboración de un documento legal que permita reflejar el cumplimiento y conocimiento de las políticas por parte del empleado, se debe requerir. El personal de esta manera no tendrán otra opción más que informarse de las políticas y acatarse a ellas.

4. Es importante conocer si el usuario entiende las políticas, principalmente aquellas que se encuentran dirigidas a sus funciones, equipos e información que maneja. Para esto no basta con tener a alguien que explique, ya que muchas veces la actitud más común que se toma cuando no se entiende es no prestar atención, por esto una solución más correcta es la de elaborar formularios breves sobre los puntos esenciales de un documento de políticas de seguridad.

5. Se puede impartir cursos sobre seguridad dirigida para diferentes audiencias (las que se observan en el documento de políticas, por ejemplo). De esta manera el personal pueden adaptarse mejor a las nuevas medidas que establecen las políticas.

6. Con el objetivo de supervisar las iniciativas que se han tomado sobre seguridad, se debe conformar un comité con supervisores o gerentes de nivel medio. Estos deben encargarse de garantizar que las actividades vigentes de seguridad están en línea con los objetivos del negocio. También tienen que preparar resúmenes de las propuestas que se presentaran a la alta gerencia acerca de los cambios que se debieran hacer sobre el documento de políticas.

7. Cada cierto tiempo se debe analizar todas las propuestas reunidas hasta este momento, y en base a estas comenzar a actualizar el documento de políticas para mantenerlo al día con los requerimientos y objetivos de la empresa. Todos los cambios que se realicen sobre el documento de políticas es importante que se den inmediatamente a conocer a todo el personal de la empresa y que nuevamente se realicen todos pasos de seguimiento sugeridos y quizás esta vez se podrían enfocar más en los cambios.

El periodo de actualización que se debe manejar sobre el documento, debería depender en primera instancia sobre el nivel de propuestas que se reúnen en la empresa. Es muy probable que al final del primer año de implementación de políticas se tengan muchas propuestas de cambios sobre el documento y que se amerite una actualización más próxima de las políticas.

Con el tiempo las políticas empezaran a resultar más acordes, las propuestas se reducirán considerablemente y se podría llegar entonces a elaborar cambios en las políticas pasando tres años que es lo aconsejable o incluso pudiera llegar a darse un máximo de cinco.

Pero lo importante es siempre tener en cuenta que las políticas es un documento que debe variar siempre por la simple razón que las tecnologías y el mundo de los negoción cambian, y con ello nuevas normas y estilos de hacer y manejar negocios ajustaran los requerimientos de la seguridad.

4.3. CONCIENTIZACIÓN DE LOS DOCUMENTOS DE POLÍTICAS

Concientizar a las audiencias es importante en el proceso de la puesta en marcha de los documentos de políticas. La importancia que la gerencia brinda a la seguridad se ve reflejada en los tópicos que se organizan dentro de la empresa para concientizar. Es difícil esperar que el personal opere

según los dictámenes que las políticas determinan si no se ha dado a conocer de manera correcta las políticas.

Las actividades que a continuación se mencionan no solo son una manera de concientizar al personal sino además son algunos pasos sugeridos que se pueden implementar para integrar mejor las políticas dentro de la organización. Algunas de estas acciones fueron tomadas del manual de "Políticas de Seguridad Informática" [1], en el cual seleccionamos las que más se apegaban al perfil de las empresas, a las cuales están dirigidos los documentos de políticas de seguridad de este proyecto.

Estas acciones serán divididas según la vía que se utilice para su distribución, en la mayoría de los casos es muy necesario distribuir la información por todos los medios aquí sugeridos, como son: En Persona, Por Escrito, En Sistemas y Por Otras Vías; ya que de esta manera no habrá excusas de que las Políticas no fueron distribuidas correctamente y puestas al conocimiento a todo el personal de la organización.

VÍA DE COMUNICACIÓN	ACCIONES
Por Escrito	• Requiera la firma en una declaración de responsabilidad personal que indique que el empleado considera el cumplimiento de las políticas como condición para mantenerse empleado. • Escriba artículos sobre seguridad para periódicos internos, boletines informativos y revistas. • Coloque anuncios y señales en las oficinas para recordar a las personas acerca de la seguridad. • Imprima rótulos y calcomanías y colóquelos en ubicaciones donde se vean, como en las copiadoras y las máquinas de fax. • Prepare un documento de la arquitectura de la seguridad informática o integre la seguridad en los planes tecnológicos de la organización. • Redacte instrucciones detalladas de respaldo e insista que el personal las cumpla. • Desarrolle y pruebe un plan de contingencia que abarque las emergencias y desastres en los sistemas • Prepare acuerdos de confidencialidad y enseñe al personal cuándo deben ser utilizados. • Prepare acuerdos de no competencia y enseñe al personal cuándo deben ser utilizados. • Prepare reportes sobre información reciente de incidentes de seguridad conjuntamente con recomendaciones para el mejoramiento de los controles.

Tabla 4. 8 Actividades que se pueden realizar por escrito.

VÍA DE COMUNICACIÓN	ACCIONES
Sistemas Electrónicos	• Conduzca evaluaciones de riesgo en seguridad informática, especialmente al hacer entrevistas y utilice otros métodos para comprometer al personal al proceso. • Solicite al departamento Legal que realice un inventario de propiedad intelectual y una evaluación de riesgos pertinente. • Emita advertencias que reflejen infracciones a las políticas. • Obsequie pequeños premios al personal ejemplar que observe las políticas y procedimientos. • Inicie un proceso de inventario de duplicación de software no autorizado donde se revisen los computadores personales para comprobar si tienen software ilegal. • Integre el adiestramiento de seguridad con otros materiales de adiestramiento en computación, como cursos para teletrabajadores, obligatorio antes de comenzar el trabajo a distancia. • Exija que el personal tome exámenes en línea para comprobar que han leído las políticas. • Prevenga el uso de servicios nuevos de sistemas, hasta que estén funcionando ciertos proyectos de seguridad. • Realice una encuesta a clientes, proveedores y terceros para conocer su nivel de confianza en la empresa.

Tabla 4. 9 Actividades que se pueden realizar a través de sistemas.

VÍA DE COMUNICACIÓN	ACCIONES
En persona	• Añada instrucciones de seguridad a programas de aplicaciones y pantallas de ayuda en los sistemas. • Antes de otorgar a los usuarios acceso a ciertas aplicaciones o facilidades en el sistema, exíjales que asistan a un breve programa de adiestramiento en línea. • Utilice software especial de identificación de vulnerabilidades para verificar los parámetros de seguridad, alertando al personal de seguridad que existen problemas. • Instale software de detección de intrusos para monitorear los intentos de entradas a los sistemas internos y usar estos reportes como evidencia para justificar mayores inversiones. • Establezca un servidor interno de Intranet y publique allí toda la información de seguridad. • Instale software para monitorear el contenido del material que pasa a través del cortafuego, e informe al personal que su comunicación está siendo monitoreada.

Tabla 4. 10 Actividades que se pueden realizar en persona.

VÍA DE COMUNICACIÓN	ACCIONES
Otras Vías	• Resuma mensajes de seguridad en bloques de notas que se suministre gratuitamente al personal. • Establezca una línea caliente con una máquina contestadora donde se puedan reportar problemas de seguridad informática de manera anónima.

Tabla 4. 11 Actividades que se pueden realizar por otras vías.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. Se pudo comprobar que con un buen análisis de riesgo, con las encuestas adecuadas, pero sobre todo con la gran colaboración del personal de las empresas, se logran definir todas las falencias que existían con respecto a la seguridad y así poder diseñar las políticas que ayuden a minimizar esas debilidades y con esto mejorar gran parte la seguridad y los procesos dentro de la empresa.

2. Con las entrevistas realizadas se comprobó que algunas empresas que recién entran al mercado de la tecnología, hablando de empresas pequeñas y/o medianas, carecen gran parte del conocimiento sobre los beneficios que brindan las políticas de seguridad y el impacto que se produce sobre el crecimiento adecuado de la empresa al no ser implementadas a tiempo.

3. Se demostró que la definición de las áreas y audiencias a las cuales estarán dirigidas las políticas desde un principio, facilita totalmente la escritura y distribución de las mismas. Logrando el entendimiento general de las políticas en todo el personal de la empresa y con ello su aceptación definitiva.

4. Se comprobó que teniendo como base los criterios de las normas ISO 17799, ISO 27000 y los del manual de “Políticas de Seguridad Informática”, se desarrollaron las políticas con las adecuadas medidas legales, evitando caer en la redundancia y politiquería por la falta de seriedad al momento de su redacción. Consiguiendo además con esto, un documento que se puede ajustar a los requerimientos de las empresas medianas.

5. Se demostró que llevando un adecuado cronograma de trabajo, donde se describan objetivos específicos a alcanzar, se logra más fácilmente culminar con éxitos el proyecto propuesto. Teniendo siempre presente separar algunos días de gracia, para algún contratiempo que pueda surgir y así no perder el objetivo planteado.

RECOMENDACIONES:

1. Dado que el tema de seguridad, es un tema sumamente importante y que requieren de mucha atención, se recomienda que antes de poner en marcha totalmente las políticas de seguridad dentro de la empresa, se establezca un departamento dedicado a este fin; es decir, un departamento de seguridad, con el personal calificado para que sean los encargados de monitorear y mejorar el cumplimiento de las políticas.

2. Es recomendable que las empresas inviten constantemente a oradores expertos en seguridad de la información, para que se dirijan al personal de toda la organización y les hablen de sus experiencias, los beneficios y ventajas que han dado las políticas de seguridad para el desarrollo de la empresa.

3. Es recomendable que se hagan de dos a tres auditorías internas, por lo menos los tres primeros años, para ir verificando hasta donde se ha ido dando el cumplimiento de las políticas y porque motivo han existido fallas en su cumplimiento. Esto ayudará, para cuando sea el momento de su actualización se tenga claro que políticas hay que mejorar más rápidamente.

ANEXOS

ANEXO A

LISTADO GENERAL DE POLÍTICAS

POLÍTICA #	TÍTULO DE LA POLÍTICA
#1	*Rol de la Información y los Sistemas informáticos.*
#2	*Esfuerzo de Equipo.*
#3	*Personas Involucradas.*
#4	*Propiedad de Archivos y Mensajes.*
#5	*Principales Departamentos que Trabajan en Seguridad de la Información.*
#6	*Tres Categorías de Responsabilidad.*
#7	*Responsabilidades del Propietario.*
#8	*Responsabilidades del Custodio.*
#9	*Responsabilidades del Usuario.*
#10	*Manejo Consistente de la Información.*
#11	*Designaciones para la Clasificación de la Información.*
#12	*Etiquetado de la Clasificación de la Información.*
#13	*Necesidad de Conocer.*
#14	*Identificadores de Usuario y Contraseñas.*
#15	*Identificadores de Usuarios Anónimos.*
#16	*Contraseñas Difíciles de Adivinar.*
#17	*Contraseñas Fáciles de Recordar.*
#18	*Patrones Repetitivos en Contraseñas.*
#19	*Restricciones de las Contraseñas.*
#20	*Almacenamiento de las Contraseñas.*
#21	*Compartir Contraseñas.*
#22	*Declaración de Conformidad.*
#23	*Divulgación de Información a Terceros.*
#24	*Solicitud de Terceros de Información de la empresa.*
#25	*Seguridad Física para Controlar el Acceso a la Información.*
#26	*Conexiones Internas de Red.*
#27	*Conexiones Externas de Red.*
#28	*Modificaciones a las Redes.*
#29	*Teletrabajo.*
#30	*Acceso a Internet.*
#31	*Correo Electrónico.*
#32	*Software antivirus.*
#33	*Erradicación de Virus.*
#34	*Respaldos Limpios.*
#35	*Fuentes de Software.*
#36	*Especificaciones Escritas para los Propietarios.*
#37	*Requisito de Autorización por Seguridad.*

POLÍTICA #	TÍTULO DE LA POLÍTICA
#38	*Control Formal de Cambios.*
#39	*Convenciones para Desarrollo de Sistemas.*
#40	*Licencias Adecuadas.*
#41	*Copias No Autorizadas.*
#42	*Responsabilidad de Respaldar.*
#43	*Protección Antirrobo.*
#44	*Divulgación de la Información de Seguridad.*
#45	*Derechos sobre el Material Desarrollado.*
#46	*Derecho a Investigar y Monitorear.*
#47	*Uso Personal.*
#48	*Conducta Inapropiada.*
#49	*Herramientas que Comprometen la Seguridad.*
#50	*Actividades Prohibidas.*
#51	*Informes Obligatorios.*
#52	*Plan de Seguridad Física*
#53	*Ubicación del Centro de Computación y Comunicaciones*
#54	*Distintivos de Identificación*
#55	*Distintivos Personales*
#56	*Entradas Individuales*
#57	*Documentación de las Aplicaciones de Producción*
#58	*Implementación de Sistemas Multiusuario*
#59	*Análisis del Impacto sobre la Seguridad Informática*
#60	*Comité de Gestión de Seguridad Informática*

CONJUNTO DE POLÍTICAS GENERALES

1. **Rol de la Información y los Sistemas Informáticos—**

   La empresa depende en forma crítica de la información y de los sistemas informáticos.
   [Véase Anexo B - 1]

   - La información debe ser protegida de acuerdo con su confidencialidad, valor y criticidad.
   - La información de la empresa debe ser usada únicamente para los propósitos de negocios expresamente autorizados por la gerencia.
   - La información es un activo vital y todos los accesos, usos y manejos de la información de la empresa deben ser consistentes con sus políticas y normas.

2. **Esfuerzo de Equipo—**

   Para que sean efectivas, las políticas de seguridad, debe constituir un esfuerzo que involucre la participación y soporte de todos los empleados de la empresa que tengan que ver con la información y los sistemas informáticos.
   [Véase: Anexo B - 2]

3. **Personas Involucradas—**

   Todo empleado de la empresa debe cumplir las políticas de seguridad que se encuentran en éste y en otros documentos correspondientes.
   [Véase: Anexo B - 3]

4. **Propiedad de Archivos y Mensajes —**

   La empresa tiene la propiedad legal del contenido de todos los archivos y mensajes almacenados o transmitidos en sus computadores y sistemas de redes, y se reserva el derecho de acceder a esta información sin aviso previo cuando exista una necesidad genuina de negocios.
   [Véase: Anexo B - 4]

5. **Principales Departamentos que Trabajan en Seguridad de la Información—**

   - El departamento de IT (o departamento técnico) es el que debe centralizar, dirigir y autorizar las actividades de seguridad de la información de todas las unidades organizacionales de la empresa.
   - El departamento de la Seguridad de la información es responsable de establecer y mantener a lo largo de toda la organización, las políticas de seguridad de la información, las normas, los lineamientos y los procedimientos.
   - El departamento de auditoría Interna es el que debe verificar y garantizar que todas las unidades organizativas están operando en forma consistente con estos requerimientos.

   [Véase: Anexo B - 5]

6. **Tres Categorías de Responsabilidad—**

   Para coordinar un esfuerzo de equipo, la empresa debe establecer tres categorías: Propietario, Custodio y Usuario. y al menos una de ellas se aplica a todo empleado.
   [Véase: Anexo B - 6]

7. **Responsabilidades del Propietario—**

   - Los propietarios de la Información deben ser responsables de la adquisición, desarrollo y mantenimiento de las aplicaciones de producción que procesan la información de la empresa.
   - Toda la información sobre los sistemas de aplicaciones de producción debe tener un propietario designado.
     [Véase: Anexo B - 7]
   - Para cada tipo de información, los propietarios deben indicar:
     - La clasificación del grado de confidencialidad,
     - Determinar el nivel apropiado de criticidad,
     - Definir cuáles usuarios recibirán el acceso, y
     - Autorizar las peticiones sobre las distintas maneras de utilizar la información.

8. **Responsabilidades del Custodio—**

   Cada clase de información contenida en los sistemas de aplicaciones de producción debe tener uno o más custodios designados. Los custodios deben:

   - Ser responsables de salvaguardar la información, incluyendo la implementación de sistemas de control de acceso para evitar la divulgación inadecuada y hacer respaldos de forma que no se pierda información crítica.
   - Implementar, operar y mantener las medidas de seguridad definidas por los Propietarios de la información.

   [Véase: Anexo B - 8]

9. **Responsabilidades del Usuario—**

   Los Usuarios deben ser responsables de conocer y cumplir todas las políticas, procedimientos y normas relativos a la seguridad de la información de la empresa.
   [Véase: Anexo B – 9]

10. **Manejo Consistente de la Información—** Se indica lo siguiente:

    - La información de la empresa, o aquélla que le ha sido confiada, debe ser protegida de manera proporcional a su nivel de confidencialidad y criticidad.
    - La información debe ser protegida en forma consistente con su clasificación, sin importar en qué fase de su ciclo de vida se encuentre, desde el origen hasta la destrucción.

    [Véase: Anexo B - 10].

11. **Designaciones para la Clasificación de la Información—**

    La información de la empresa debe ser dividida en cuatro grupos: Secreta, Confidencial, Uso Interno Solamente o Pública. Todos los empleados deben familiarizarse con las definiciones de estas categorías y con los pasos a seguir para proteger la información que corresponde a estas categorías. [Véase: Anexo B - 11]

12. **Etiquetado de la Clasificación de la Información—**

    Si la información es sensible, desde el momento en que es creada hasta el momento en que es destruida o desclasificada, debe ser etiquetada con una designación apropiada de clasificación de información. Este tipo de marcas deben aparecer en todas las manifestaciones de la información.
    [Véase: Anexo B - 12]

13. **Necesidad de Conocer—**

El acceso a la información en posesión o bajo el control de la empresa debe proporcionarse de acuerdo al concepto de la necesidad de conocer.

- La información debe ser divulgada únicamente a aquellas personas que tienen una necesidad legítima que se deriva de asuntos de negocios. Al mismo tiempo, los empleados no deben negar el acceso a información cuando el propietario exige u ordena que sea compartida.
- Los empleados no deben intentar acceder a información sensible a menos que el propietario les haya dado el derecho al acceso.
- Cuando un empleado cambia sus responsabilidades, incluyendo cese laboral, transferencia, promoción y permiso remunerado, su supervisor debe notificar inmediatamente al departamento de seguridad de la información o al asignado por la empresa.
- Los privilegios que se otorgan a todos los empleados deben ser revisados periódicamente por los propietarios y custodios para garantizar que únicamente aquéllos con necesidad actual de conocimiento tengan acceso a la información.

[Véase: Anexo B - 13]

14. **Identificadores de Usuario y Contraseñas—**

La utilización de usuarios y contraseñas deben ser implementadas teniendo presente:

- Todo empleado que accede a sistemas informáticos multiusuario debe tener un único identificador y una contraseña
  [Véase: Anexo B - 14].
- Estos identificadores de usuario deben ser empleados para restringir los privilegios informáticos con base en las responsabilidades del trabajo, del proyecto y de otras actividades de negocios.
- Cada empleado debe ser responsable por el uso de su identificador y contraseña.

15. **Identificadores de Usuarios Anónimos—**

- Con excepción de los boletines electrónicos, sitios de Internet, sitios de Intranet y otros sistemas en los que los usuarios regulares permanecen anónimos, los usuarios tienen prohibido conectarse a cualquier sistema o red de la empresa en forma anónima.
- Cuando los usuarios emplean comandos del sistema que les permiten cambiar identificadores de usuarios activos para obtener ciertos privilegios, deben haberse conectado inicialmente empleando identificadores de usuarios que claramente indican sus identidades.

[Véase: Anexo B - 15]

16. **Contraseñas Difíciles de Adivinar—**

Los usuarios deben escoger contraseñas que sean difíciles de adivinar. Esto significa que:

- Las contraseñas no pueden estar relacionadas con su trabajo o con su vida privada,
- Las contraseñas no deben ser palabras que se encuentran en diccionarios o cualquier parte gramatical.

[Véase: Anexo B - 16]

17. **Contraseñas Fáciles de Recordar—**

Los usuarios deben escoger contraseñas fáciles de recordar que al mismo tiempo sean difíciles de adivinar por terceros no autorizados si realizan algún método de descubrimiento de contraseña.
[Véase: Anexo B - 17].

18. **Patrones Repetitivos en Contraseñas—**

- Los usuarios no deben construir contraseñas usando una secuencia básica de caracteres que cambia parcialmente en función de la fecha o de otro factor predecible.
- Los usuarios no deben construir contraseñas que son idénticas o sustancialmente similares a contraseñas que hayan utilizado con anterioridad.

19. **Restricciones de las Contraseñas—**

- Las contraseñas deben tener al menos 10 caracteres de longitud.
- Las contraseñas deben ser cambiadas cada 90 días o a intervalos más frecuentes.
- Cuando un empleado sospecha que su contraseña la conoce otra persona, debe cambiarla inmediatamente.

20. **Almacenamiento de las Contraseñas—**

- Las contraseñas no deben almacenarse en forma legible en:
  - Archivos por lotes,
  - Comandos para acceso automático,
  - Macros de software,
  - Teclas de función,
  - En computadores que no posean sistemas de control de acceso,
  - En cualquier otra ubicación en donde personas no autorizadas puedan descubrirlas.
- Tampoco deben escribirse en una forma fácilmente descifrable y dejarse en un lugar en el que puedan ser descubiertas por personas no autorizadas.

21. **Compartir Contraseñas—**

- Las contraseñas nunca deben compartirse ni revelarse a otros.
- Los administradores del sistema y el equipo técnico de sistemas informáticos nunca deben pedirle a un empleado que revele su contraseña.
- Únicamente cuando se crea la contraseña podría ser conocida por otro. Estas contraseñas temporales deben ser cambiadas la primera vez que el usuario autorizado accede al sistema.
- Si el usuario sospecha que su identificador de usuario y contraseña han sido utilizados por alguien más, debe notificarlo inmediatamente al administrador del sistema informático.

22. **Declaración de Conformidad—**

- Todos los empleados que deseen utilizar los sistemas de computadores multiusuario de la empresa deben firmar una declaración de conformidad antes de que se les otorgue el identificador de usuario.
- Cuando ya poseen identificadores de usuario, deben firmar la declaración antes de recibir la renovación anual de sus identificadores de usuario.

[Véase: Anexo B - 18]

23. **Divulgación de Información a Terceros—**

- A menos que haya sido específicamente designada como pública, toda la información interna de la empresa debe ser protegida contra su divulgación a terceros.
- Únicamente se debe dar a conocer la información a Terceros si existe y es demostrable la necesidad de conocer, cuando se ha firmado un acuerdo de sensibilidad y cuando esta divulgación ha sido expresamente autorizada por el propietario relevante de la información de la empresa.
- Si se pierde o se sospecha de la pérdida o divulgación a terceros no autorizados de información sensible, el propietario de la información y el departamento de seguridad de la información (o departamento de IT) deben ser notificados inmediatamente.

24. **Solicitud de Terceros de Información de la empresa—**

- A menos que el empleado haya sido autorizado por el propietario de la información para divulgarla públicamente, todas las solicitudes de información acerca de la empresa y su negocio deben ser dirigidas al departamento de relaciones públicas o al departamento que asigne la gerencia. [Véase: Anexo B - 19]
- Si un empleado recibe información sensible desde terceros en beneficio de la empresa, esta recepción debe estar precedida de la firma de este tercero de un formulario de liberación de la empresa.

25. **Seguridad Física para Controlar el Acceso a la Información—**

- Debe restringirse el acceso físico a cualquier oficina, sala de computadores u otra área de trabajo de la empresa que contenga información sensible.
- Cuando no es utilizada la información sensible, siempre debe estar protegida contra la divulgación no autorizada.
- La información sensible en papel debe guardarse bajo llave en contenedores apropiados cuando se deja en una oficina sin vigilancia. [Véase: Anexo B - 20].
- Fuera del horario de trabajo, los empleados que trabajan en áreas que contienen información sensible deben guardar bajo llave toda la información.
- A menos que la información esté siendo utilizada por personal autorizado, los escritorios deben mantenerse limpios y sin documentos fuera del horario de trabajo para evitar el acceso no autorizado a la información.
- Los empleados deben colocar las pantallas de sus computadores en una posición en la que se evite que personal no autorizado pueda ver la información sensible que se encuentre desplegada en ellas.

26. **Conexiones Internas de Red—**

- Todos los computadores de la empresa que almacenan información sensible y que están permanente o intermitentemente conectados a las redes internas, deben tener un sistema de control de acceso mediante contraseñas aprobadas por el departamento de seguridad informática o el departamento que asigne la gerencia.
- Al margen de las conexiones de red, todos los computadores no conectados que manejan información sensible, deben tener un sistema aprobado de control de acceso con contraseñas.
- Los usuarios que trabajan con otras clases de computadores deben emplear las contraseñas del protector de pantalla provistas por los sistemas operativos, de forma tal que después de un período de inactividad, la información en pantalla desparezca hasta que se introduzca la contraseña apropiada.
- Los sistemas multiusuario a lo largo de la empresa deben emplear sistemas de desconexión automática que finalizan la sesión del usuario después de un determinado período de inactividad.

27. **Conexiones Externas de Red—**

- Todas las sesiones entrantes de conexión a los computadores de la empresa desde redes externas deben estar protegidas con un sistema autorizado de control de acceso mediante contraseñas dinámicas. [Véase Anexo B - 21]
- Los usuarios con computadores personales conectados a redes externas tienen prohibido mantenerse conectados mientras funcione el software de comunicación de datos, a menos que previamente se haya instalado un sistema autorizado de contraseñas dinámicas.
- Cuando usen los computadores de la empresa, los empleados no pueden establecer conexiones con redes externas, incluyendo proveedores de servicios de Internet, a menos que estas conexiones hayan sido autorizadas por el departamento de Seguridad Informática o el que asigne la gerencia.

28. **Modificaciones a las Redes—**

- Con excepción de situaciones de emergencia, todos los cambios en las redes computarizadas de la empresa deben estar documentados en una orden de trabajo y autorizados previamente por el departamento de técnico o de IT.
- Todos los cambios de emergencia a las redes de la empresa deben ser efectuados únicamente por personas autorizadas por el departamento técnico o de IT.
  [Véase: Anexo B - 22]

29. **Teletrabajo—**

A discreción de la gerencia, el permiso para que cierto personal calificado pueda llevar trabajo a su casa, solo debe ser otorgado por el supervisor inmediato de cada empleado en función de un listado de verificación de factores relevantes. [Véase: Anexo B - 23]

30. **Acceso a Internet—**

Los empleados están provistos de acceso a Internet para llevar a cabo sus tareas, pero este acceso puede darse por terminado en cualquier momento a discreción del supervisor inmediato del empleado.

- El acceso a Internet debe ser monitoreado para asegurar que los empleados no visiten sitios no relacionados con su trabajo y también para garantizar el cumplimiento de las políticas de seguridad.
- Los empleados deben tener especial cuidado en no representar a la empresa en grupos de discusión por Internet o en otros foros públicos, a menos que hayan recibido previamente autorización de la alta gerencia para así hacerlo.
- Toda la información que se recibe de Internet debe ser considerada sospechosa hasta que se confirme con fuentes confiables.
- Los empleados no deben colocar material de la empresa en sistemas de computación accesibles públicamente como por ejemplo Internet, a menos que haya sido aprobado tanto por el propietario de la información como por el departamento de tecnología Informática.
- Los usuarios tienen prohibido efectuar transacciones de comercio electrónico por Internet a menos que el departamento técnico o de IT hayan aprobado este tipo de actividades.
- La información sensible, incluyendo contraseñas y números de tarjetas de crédito, no debe ser enviada a través de Internet a menos que se encuentre cifrada. [Véase: Anexo B - 24].

31. **Correo Electrónico—**

- Todo trabajador de la empresa que utiliza computadores debe recibir una dirección de correo electrónico con sus privilegios correspondientes.
- En todas las comunicaciones de la empresa, que envíe o reciba por correo electrónico, debe utilizar esta dirección de correo electrónico de la compañía.
- No debe utilizar para actividades de negocios de la empresa una dirección electrónica de correo personal de un proveedor de servicios de Internet a menos que reciba la autorización de la gerencia.
- No se debe transmitir correo electrónico no solicitado a clientes o prospectos.
- No se debe enviar mensajes emotivos y sobrecargar la cuenta de correo electrónico con grandes cantidades de mensajes.

- Todas las comunicaciones de trabajo transmitidas por correo electrónico deben ser revisadas por el supervisor inmediato antes de enviarse y tener una apariencia y tono profesional y de negocios.
- Los trabajadores de la empresa deben abstenerse de enviar números de tarjetas de crédito, contraseñas o cualquier otra información confidencial que pueda ser interceptada.
- Todo el personal de la empresa debe emplear una firma normalizada de correo electrónico que incluya su nombre completo, cargo, dirección de trabajo y número telefónico del trabajo.
- Los usuarios no deben almacenar mensajes importantes en la bandeja de entrada.

32. **Software antivirus—**

- Todos los usuarios de computadores personales deben tener versiones actualizadas de software antivirus ejecutándose en sus computadores.
- Los usuarios no deben abortar procesos automáticos de actualización de antivirus.
- El software antivirus debe utilizarse para revisar todos los archivos y programas provenientes de terceros o de otros grupos de la empresa.
- Los trabajadores no deben dejar de utilizar o desactivar el proceso de revisión que podría evitar la transmisión de un virus.

33. **Erradicación de Virus—**

- Si los trabajadores sospechan que el computador está infectado con un virus, deben dejar de utilizarlo inmediatamente y llamar al Centro de Atención al Usuario.
- No deben intercambiarse ningún tipo de memorias portátiles ni otros medios de almacenamiento entre el computador infectado y otros computadores hasta que el virus haya sido exitosamente erradicado.
- El computador infectado debe ser inmediatamente aislado de las redes internas.
- Los usuarios no deben intentar erradicar los virus por sí mismos.
- El personal calificado de la empresa o consultores deben llevar a cabo la tarea de erradicación de Virus de manera que se minimicen tanto la destrucción de los datos como el tiempo de caída del sistema.

34. **Respaldos Limpios**—

Todos los programas de los computadores personales deben ser copiados antes de ser utilizados por primera vez y estas copias deben almacenarse en lugares seguros, como un gabinete bajo llave, indicado por el encargado del departamento técnico o de IT. [Véase: Anexo B - 25].

35. **Fuentes de Software**—

- Los computadores y redes de la empresa no deben ejecutar programas que provengan de fuentes distintas de:
  - Los departamentos de la empresa,
  - Los usuarios conocidos y confiables,
  - Las autoridades reconocidas de sistemas de seguridad, o,
  - Los proveedores establecidos de computadores, redes o software.
- No deben utilizarse los programas que se descargan de boletines electrónicos, dominios públicos y otras fuentes no confiables a menos que hayan sido objeto de rigurosas pruebas aprobadas por el departamento técnico o de IT.

36. **Especificaciones Escritas para los Propietarios**—

Todos los programas desarrollados internamente, para procesar información crítica o sensible de la empresa, deben tener una especificación formal por escrito. [Véase: Anexo B - 26].

37. **Requisito de Autorización por Seguridad—**

Antes de utilizar aplicaciones nuevas o sustancialmente modificadas en el procesamiento de producción, debe existir una autorización escrita del departamento de IT con relación a los controles que deben emplearse. [Véase: Anexo B - 27].

38. **Control Formal de Cambios—**

Todos los computadores y sistemas de comunicación utilizados para el procesamiento de producción deben emplear un proceso documentado de control de cambios, de forma tal que se garantice que solamente se realicen cambios autorizados. [Véase: Anexo B - 28].

39. **Convenciones para Desarrollo de Sistemas—**

Todas las actividades de desarrollo de software de producción y de mantenimiento llevadas a cabo internamente deben cumplir las políticas, normas y procedimientos del departamento Técnico o de IT y demás convenciones de desarrollo de sistemas. [Véase: Anexo B - 29].

40. **Licencias Adecuadas—**

- La gerencia de la empresa debe hacer arreglos adecuados con los proveedores de software para obtener copias adicionales con licencia en caso de que éstas sean necesarias para actividades de negocios.
- Todos los programas deben ser adquiridos a través del departamento de Compras o el indicado por la gerencia.

41. **Copias No Autorizadas—**

Los usuarios no deben copiar los programas suministrados por la empresa en ningún medio de almacenamiento, transferir dichos programas a otro computador ni hacerlos públicos a terceros sin el permiso previo de su supervisor, con la excepción de copias de respaldo. [Véase: Anexo B - 30].

42. **Responsabilidad de Respaldar—**

- Los usuarios de computadores personales deben respaldar con regularidad la información almacenada en sus computadores o asegurarse de que alguien lo haga por ellos.
- En el caso de computadores multiusuario y sistemas de comunicación, el administrador del sistema debe realizar respaldos periódicos.
- Si es solicitado, el departamento de tecnología informática debe instalar o proveer asistencia técnica para la instalación de dispositivos de hardware y software para respaldos.
- Todos los respaldos que contengan información crítica o confidencial deben ser almacenados en una ubicación aprobada fuera del sitio de respaldo, en donde existan controles de acceso físico o cifrado.
- Debe prepararse un plan de contingencia para todas las aplicaciones que manejan información crítica de producción.
- El Propietario de la información debe garantizar que este plan se desarrolle adecuadamente, que se actualice regularmente y que se pruebe periódicamente.

43. **Protección Antirrobo—**

- Todos los computadores y redes de la empresa deben estar físicamente asegurados con dispositivos antirrobo en caso de que se encuentren en una oficina de libre acceso.
- Los servidores de redes locales y otros sistemas multiusuario deben colocarse en gabinetes, armarios o salones de computación bajo llave.
- Los computadores portátiles que se encuentren en una oficina de libre acceso y que no se estén usando también deben estar asegurados con cables bloqueadores, colocados en gabinetes cerrados o asegurados con cualquier otro sistema de bloqueo.
- Los equipos de redes y computación no deben ser removidos de las oficinas de la empresa, a menos que la persona que quiera hacerlo haya obtenido la autorización de la gerencia del edificio.

44. **Divulgación de la Información de Seguridad—**

La información acerca de las medidas de seguridad para los computadores y sistemas de red de la empresa es confidencial y no debe ser divulgada a personas que no sean usuarios autorizados de dichos sistemas a menos que lo autorice el director del departamento técnico o de IT.
[Véase: Anexo B - 31].

45. **Derechos sobre el Material Desarrollado—**

Mientras los trabajadores desempeñen labores para la empresa, deben ceder a ésta los derechos exclusivos sobre patentes, derechos de autor, de invenciones o de propiedad intelectual de todo lo que creen o desarrollen. [Véase: Anexo B - 32].

46. **Derecho a Investigar y Monitorear—**

La gerencia de la empresa se reserva el derecho de monitorear, inspeccionar o investigar en cualquier momento todos sus sistemas informáticos.

- Todas las búsquedas de esta naturaleza deben llevarse a cabo después de obtener la autorización de los departamentos Legal y Técnico o de IT.
- Debido a que los computadores y redes de la empresa son proporcionados únicamente con fines de negocios, los trabajadores no deben esperar que exista privacidad en la información que almacenen o envíen a través de estos sistemas informáticos.
- La gerencia de la empresa tiene el derecho de eliminar de sus sistemas informáticos cualquier material que considere ofensivo o potencialmente ilegal.
  [Véase: Anexo B - 33]

47. **Uso Personal—**

- Los sistemas informáticos de la empresa deben ser utilizados únicamente con fines de negocios.
- No se deben utilizar juegos que se encuentren en paquetes de software independientes.
- No se deben utilizar los sistemas informáticos de la empresa, para enviar cadenas de cartas, peticiones de caridad, material de campañas políticas, trabajo religioso, para la transmisión de material objetable o cualquier otro uso con fines no relacionados con el negocio.
  [Véase: Anexo B - 34].

48. **Conducta Inapropiada—**

La gerencia de la empresa se reserva el derecho de revocar los privilegios informáticos a cualquier usuario en cualquier momento.
[Véase: Anexo B – 35]

49. **Herramientas que Comprometen la Seguridad—**

- A menos que hayan sido expresamente autorizados por el departamento técnico o de IT, los trabajadores de la empresa no deben adquirir, poseer, comerciar o utilizar herramientas de hardware o software que puedan ser empleadas para evaluar o comprometer la seguridad de los sistemas informáticos.
- Sin la autorización dada por el departamento de técnico o de IT, los trabajadores no deben utilizar cualquier clase de hardware o software que monitoree el tráfico en una red o las actividades de un computador.
  [Véase: Anexo B - 36]

50. **Actividades Prohibidas—**

- Los usuarios no deben examinar o intentar comprometer las medidas de seguridad de los computadores o sistemas de comunicación, a menos que hayan sido previamente autorizados por escrito por el director del departamento de auditoría interna.
- Los incidentes que involucren actividades no autorizadas en el sistema, adivinado de contraseñas, descifrado de archivos, contrabando de copias de software, o cualquier otro intento similar de comprometer las medidas de seguridad, pueden ser ilegales y deben considerarse como una seria violación de la política interna de la empresa.
  [Véase: Anexo B - 37]

51. **Informes Obligatorios—**

Todas las violaciones de políticas de las que se tenga sospecha, intrusiones en el sistema, contaminaciones por virus o cualquier otra condición que pueda amenazar la información o los sistemas informáticos de la empresa, deben ser inmediatamente informadas al departamento técnico o de IT. [Véase: Anexo B - 38]

52. **Plan de Seguridad Física—**

Todo centro de datos de la empresa debe tener un plan de seguridad física que debe ser revisado y actualizado anualmente por el gerente a cargo de las instalaciones.

53. **Ubicación del Centro de Computación y Comunicaciones—**

Los computadores multiusuario y las instalaciones de comunicaciones deben estar ubicados más arriba de un primer piso, alejados de cocinas y en una ubicación separada de las paredes exteriores del edificio mediante una pared interna, en un salón sin ventanas.
[Véase: Anexo B - 39]

54. **Distintivos de Identificación—**

Mientras se encuentren dentro de las instalaciones o edificios seguros de la empresa, las personas deben portar sus dispositivos de identificación de tal manera que la foto y la información sean claramente visibles.

55. **Distintivos Temporales—**

Los trabajadores que hayan olvidado traer sus distintivos de identificación deben obtener un distintivo temporal válido por un día, a cambio de su licencia de conducir o cualquier otra identificación con foto.

56. **Entradas Individuales—**

Todas las entradas de tráfico peatonal a todos los centros de datos de la empresa deben tener mecanismos de trampas humanas.
[Véase: Anexo B - 40]

57. **Documentación de las Aplicaciones de Producción—**

Antes de mover la aplicación hacia un ambiente de producción, el propietario correspondiente de la información debe haber preparado y autorizado la documentación para todas las aplicaciones de producción, lo cual incluye una lista de los recursos de sistemas que deben ejecutarse, una lista de los archivos utilizados y afectados, una lista de los aspectos de seguridad, una descripción de las formas en que el flujo de trabajo se va a monitorear, y una descripción de la forma de cómo será manejado el producto resultante.

58. **Implantación de Sistemas Multiusuario—**

Los trabajadores no deben instalar servidores para la intranet, ni foros electrónicos, ni redes de área local, ni conexiones con módems a redes internas ya existentes, ni otros servicios multiusuario para transmitir información sin la autorización específica del jefe del departamento de seguridad informática, sino no existe éste el jefe del departamento técnico.

59. **Análisis del Impacto sobre la Seguridad Informática—**

Cada vez que se vaya a cargar información sensible en los computadores, o a utilizarse de maneras sustancialmente nuevas y diferentes, se debe llevar a cabo una evaluación de riesgo de los impactos potenciales sobre la seguridad.

60. **Comité de Gestión de Seguridad Informática—**

Un comité gerencial de seguridad de la información, compuesto por la alta gerencia o sus delegados de cada división principal de la empresa, debe reunirse trimestralmente para revisar el nivel actual de seguridad de la información, revisar los procesos de monitoreo de los incidentes de seguridad de la empresa, aprobar y luego revisar los proyectos de seguridad de la información, aprobar políticas nuevas o modificadas y realizar otras actividades gerenciales de alto nivel necesarias para mantener la seguridad de la información.

ANEXO B

ACLARACIONES Y ESPECIFICACIONES DE LAS POLÍTICAS

1. **De Anexo A – Política 1.** Si se revela información importante a personas inapropiadas, la empresa puede sufrir pérdidas considerables o salir del negocio.
   La buena reputación de la empresa está directamente relacionada con la manera en que maneja tanto la información como los sistemas informáticos.
   Por ejemplo, si se hace pública información confidencial de un cliente, la reputación de la empresa se vería afectada.
   Por ésta y otras importantes razones de negocio, la gerencia ejecutiva en conjunto con la junta directiva ha iniciado y continúa manteniendo un esfuerzo de seguridad informática.
   Parte de este esfuerzo es la definición de estas políticas de seguridad informática.

2. **De Anexo A – Política 2.** Al reconocer la necesidad de un equipo de trabajo, esta declaración establece las responsabilidades de los usuarios y los pasos que deben seguir a fin de ayudar a proteger la información y los sistemas informáticos de la empresa.

3. **De Anexo A – Política 3.** Los empleados que deliberadamente violen ésta y otras declaraciones sobre políticas de seguridad estarán sujetos a acciones disciplinarias que pueden incluir el cese de sus funciones.

4. **De Anexo A – Política 4.** Se desea disuadir en los empleados, la aclaración de que los sistemas en la empresa no son para fines personales. Además, de facilitar el proceso de análisis de los archivos de correo electrónico y los directorios de archivos de computadores personales que los usuarios podrían de otra manera considerar confidenciales y privados.

5. **De Anexo A – Política 5.** La investigación sobre intrusiones en el sistema y otros incidentes de seguridad de la información deben ser responsabilidad del departamento de IT. Las sanciones disciplinarias resultantes de las violaciones a los requerimientos de seguridad serán manejadas por los gerentes locales. Esta distribución y obligación está sujeta a cambios según los departamentos existentes en la empresa.

6. **De Anexo A – Política 6.** Estas categorías definen las responsabilidades generales con respecto a la seguridad de la información. Las cuales se definen en las siguientes políticas

    - **Responsabilidades del Propietario**
    - **Responsabilidades del Custodio**
    - **Responsabilidades del Usuario**

    Véase: Anexo A – Políticas 7, 8, 9.

7. **De Anexo A – Política 7.** Las aplicaciones de producción son programas computarizados que regularmente proveen informes que soportan la toma de decisiones y otras actividades de negocios.

    Los propietarios de la información son:

    - Los gerentes de departamento,
    - Los integrantes de la alta gerencia, o
    - Los delegados dentro de la empresa.

8. **De Anexo A – Política 8.** Los Custodios tienen la posesión física o lógica de la información de la empresa o de aquélla que ha sido confiada a la empresa. Si bien los integrantes del equipo del departamento de tecnología informática son claramente custodios, también lo son los administradores del sistema local; y, cuando la información se mantiene solamente en un computador personal, el Usuario también es un custodio.

9. **De Anexo A – Política 9.** Los usuarios que tengan preguntas acerca del manejo adecuado de un tipo específico de información deben ser dirigidas directamente al custodio o al propietario de dicha información.

10. **De Anexo A – Política 10.** Deben emplearse medidas de seguridad sin importar el medio en que ha sido almacenada la información, los sistemas que la procesan o los métodos a través de los cuales es transportada.

11. **De Anexo A – Política 11.** Toda la información bajo el control de la empresa, sea generada interna o externamente, se encuentra en alguna de estas categorías. Pero, estas designaciones de clasificación están sujetas a cambios y no necesariamente deben existir los cuatro grupos, todo depende de los requerimientos de la empresa.

12. **De Anexo A – Política 12.** La gran mayoría de la información de la empresa corresponde a la categoría de Uso Interno Solamente. Por esta razón, no es necesario etiquetarla. La información que no es etiquetada por descarte se clasifica como Uso Interno Solamente.

13. **De Anexo A – Política 13.** El concepto de Necesidad de Conocer, comprende el hecho de definir bajo qué condiciones y requisitos la información puede ser dada a conocer. Especifica los controles de acceso y privilegios que se tiene sobre la información de la empresa. Para implementar el concepto de necesidad de conocer, la empresa adopta un proceso de solicitud de acceso y autorización por parte del propietario.

14. **De Anexo A – Política 14.** El acceso a sistemas informáticos multiusuario con un único identificador y una contraseña, es uno de los procesos de Necesidad de Conocer que puede implementar la empresa.

15. **De Anexo A – Política 15.** El acceso anónimo podría, por ejemplo, involucrar el uso de identificadores de usuarios "invitados".

16. **De Anexo A – Política 16.** Relacionadas a su trabajo o vida privada, por ejemplo, no pueden utilizarse el número de placa del automóvil, el nombre del cónyuge o partes de una dirección. Relacionadas al diccionario, por ejemplo, no deben usarse nombres propios, lugares, términos técnicos o expresiones comunes.

17. **De Anexo A – Política 17.** Métodos Posibles de descubrimiento de contraseña:

    - Reúnen varias palabras en una sola.
    - Mueven una palabra una fila hacia arriba, abajo, izquierda o derecha en el teclado.
    - Mueven los caracteres de una palabra un número determinado de letras hacia arriba o abajo en el alfabeto.
    - Transforman una palabra de acuerdo con un método específico, como convertir una letra en un número que refleja su posición dentro de la palabra.
    - Combinan puntuación o números en una palabra.
    - Forman acrónimos de palabras de canciones, poemas u otra secuencia conocida de palabras.
    - Escriben mal una palabra deliberadamente.
    - Combinan algunas preferencias como el horario preferido de acostarse y los colores favoritos.

18. **De Anexo A – Política 22.** La firma de la declaración de conformidad indica que el usuario involucrado comprende y conviene en adherirse a las políticas y procedimientos de la empresa relacionados con los *computadores y redes,* incluyendo las instrucciones contenidas en la política del Anexo A - 22.

19. **De Anexo A – Política 24.** Estas solicitudes incluyen cuestionarios, investigaciones y entrevistas por la prensa. Esta política no se aplica a la información de ventas y mercadeo de los productos y servicios de la empresa X ni se refiere a las llamadas de soporte técnico de los clientes.

20. **De Anexo A – Política 25.** Si el Custodio de este tipo de información considera que estará fuera por menos de 30 minutos, la información en papel puede dejarse sobre el escritorio o en cualquier otro lugar visible sólo si todas las puertas y ventanas de la oficina se encuentran cerradas bajo llave.

21. **De Anexo A – Política 27.** Las contraseñas dinámicas son diferentes cada vez que se usan, por lo que no deben ser reutilizadas para obtener acceso no autorizado.

22. **De Anexo A – Política 28.** Este proceso evita cambios inesperados que puedan conducir a la negación de algún servicio, divulgación no autorizada de información y otros problemas. Este proceso se aplica no solamente a los empleados sino también al personal de ventas.

23. **De Anexo A – Política 29.** El permiso permanente de llevar trabajo a casa depende parcialmente de la continua conformidad con ciertas políticas de seguridad informática y normas. El chequeo periódico del correo electrónico en la vía desde o hacia la casa no se considera como llevar trabajo a casa, sin embargo, requiere que los empleados tomen las mismas precauciones de seguridad.

24. **De Anexo A – Política 30.** La creación de páginas en Internet es manejada en forma independiente mediante un proceso de aprobación que involucra al comité de comunicaciones externas o aquellos determinados por la gerencia.

25. **De Anexo A – Política 34.** Las copias maestras no deben ser utilizadas en las actividades cotidianas del negocio sino ser guardadas, en caso de recuperación por infecciones de virus, fallas del disco duro y otros problemas.

26. **De Anexo A – Política 36.** Las especificaciones escritas para los propietarios debe incluir una discusión sobre riesgos de seguridad y controles como sistemas de control de acceso y planes de contingencia. La especificación debe formar parte de un acuerdo entre el propietario de la información y el desarrollador del sistema. En este caso no se consideran programas las macros para hojas de cálculo y los documentos elaborados en procesadores de palabras.

27. **De Anexo A – Política 37.** El requisito de Autorización por Seguridad se aplica tanto a computadores personales como a sistemas más grandes.

28. **De Anexo A – Política 38.** El procedimiento de Control Formal de Cambios mencionado en el Anexo A, política 38 debe utilizarse para todos los cambios significativos en los sistemas de producción, hardware, enlaces de comunicación y procedimientos. Esta política se aplica a los computadores personales en donde se ejecutan sistemas de producción y en grandes sistemas multiusuario.

29. **De Anexo A – Política 39.** Las convenciones de desarrollo de sistemas incluyen la correcta verificación, adiestramiento y documentación.

30. **De Anexo A – Política 41.** Las copias de respaldo mencionadas, están contempladas en el Anexo A, política 34.

31. **De Anexo A – Política 44.** Ejemplo, está prohibido publicar en directorios los números telefónicos del módem u otra información de acceso a los sistemas. Se permite la publicación de direcciones de correo electrónico.

32. **De Anexo A – Política 45.** Todos los programas y documentación generados o provistos por los trabajadores para beneficio de la empresa son propiedad de la empresa. La empresa tiene la propiedad sobre los contenidos de todos los sistemas informáticos bajo su control. La empresa se reserva el derecho de acceder y utilizar esta información a su discreción.

33. **De Anexo A – Política 46.** Este examen puede hacerse con o sin el consentimiento, presencia o conocimiento de los trabajadores correspondientes. Los sistemas informáticos que estén sujetos a este tipo de examen incluyen, pero no se limitan a los archivos del sistema de correo electrónico, archivos en el disco duro del computador personal, archivos de correo de voz, archivos a imprimir, documentos recibidos de la máquina de fax, las gavetas de los escritorios y las áreas de almacenamiento.

34. **De Anexo A – Política 47.** El uso personal de los sistemas informáticos en forma incidental, es permisible si no consume más que un número trivial de recursos que podrían de otra manera ser:

    - Utilizados con propósitos de negocios,
    - Si no interfiere con la productividad del trabajador, y
    - No está en contra de cualquier actividad de negocios.

    El uso incidental permisible del sistema de correo electrónico podría involucrar, por ejemplo, el envío de un mensaje para planificar un almuerzo. El uso personal que no se encuentre en estas tres categorías debe ser autorizado previamente por el gerente del departamento. Los juegos computarizados que se encuentren en los sistemas operativos pueden usarse durante los recesos o la hora de almuerzo, siempre que esta actividad no interfiera con la productividad del trabajador.

35. **De Anexo A – Política 48.** No es permisible la conducta que interfiera con la normal y adecuada operación de los sistemas informáticos de la empresa que adversamente afecte la capacidad de otros de utilizar estos sistemas informáticos o que sea dañina u ofensiva para otros.

36. **De Anexo A – Política 49.** Pueden ser ejemplos de estas herramientas de hardware o software, aquéllas que frustran la protección de copiado de programas, descubren contraseñas secretas, identifican vulnerabilidades en la seguridad o descifran archivos cifrados.

37. **De Anexo A – Política 50.** Están absolutamente prohibidos los atajos que circunden las medidas de seguridad, las travesuras y bromas prácticas que comprometan las medidas de seguridad de los sistemas.

38. **De Anexo A – Política 51.** El aviso puede hacerse vía correo electrónico o de voz, según el indicado por el departamento de IT. Los mensajes dejados en estos buzones de correo pueden ser anónimos.

39. **De Anexo A – Política 53.** En el caso de no cumplir con las condiciones físicas para cumplir en su totalidad lo estipulado en la política, el gerente a cargo debe instalar otros controles que reduzcan o eliminen las pérdidas, aun cuando la ubicación del centro de computación no se modifique.

40. **De Anexo A – Política 56.** Al requerir que las personas pasen a través de puertas controladas, uno por uno, la organización impide que se entre en grupos. A pesar de que un torniquete puede ser utilizado para este propósito, la trampa humana individual suministra una medida de control adicional donde un intruso puede quedar encerrado hasta que llegue el personal de seguridad. Una trampa humana también puede ser configurada para que las personas salgan del área individualmente.

ANEXO C

ENCUESTA PARA LA REALIZACIÓN DE POLÍTICAS DE SEGURIDAD

SE PERMITE MAS DE UNA RESPUESTA A MENOS QUE SE INDIQUE LO CONTRARIO.

1. **¿A QUÉ SE DEDICA LA EMPRESA?**
   - ☐ a) Proveer servicio de internet
   - ☐ b) Proveer servicio de correos electrónicos
   - ☐ c) Proveer servicios de seguridad
   - ☐ d) Proveer servicios técnicos
   - ☐ e) Proveer servicio de hosting
   - ☐ f) OTROS:_____

2. **INDIQUE LOS DEPARTAMENTOS QUE POSEE LA EMPRESA**
   - ☐ a) Departamento gerencial y/o administrativo
   - ☐ b) Departamento de recursos humanos o personal
   - ☐ c) Departamento de Marketing y/o Comercial o Ventas
   - ☐ d) Departamento técnico o grupo de IT
   - ☐ e) Departamento de seguridad
   - ☐ f) OTROS:_____

3. **¿LA EMPRESA POSEE O SE BASA EN ALGÚN TIPO DE POLÍTICAS DE SEGURIDAD ESTANDAR?**
   - ○ a) Sí, propias de la empresa
   - ○ b) Sí, basadas en algún estándar (Cual:_____)
   - ○ c) No (Pase a la pregunta 11)

4. **¿QUIÉN ES EL ENCARGADO DE CONTROLAR EL CUMPLIMIENTO DE SUS POLÍTICAS?**
   - ☐ a) Jefe de departamento técnico
   - ☐ b) Personal de departamento técnico
   - ☐ c) Jefe de departamento de seguridad
   - ☐ d) Personal de departamento de seguridad
   - ☐ e) Jefe o persona asignada por cada departamento
   - ☐ f) OTROS:_____

5. **¿HAN TENIDO ALGÚN PROBLEMA CON EL CUMPLIMIENTO DE LAS POLÍTICAS?**
   - ○ a) Sí
   - ○ b) No

6. **¿CUÁL HA SIDO LA RAZÓN POR LA FALTA DE INCUMPLIMIENTO DE LAS POLÍTICAS?**
   - ☐ a) Por definición incorrecta de la política
   - ☐ b) Rechazo de la política
   - ☐ c) Incorrecta distribución de las políticas
   - ☐ d) OTROS:_____

7. **¿QUÉ DEPARTAMENTO HA TENIDO MAS PROBLEMAS EN EL CUMPLIMIENTO DE LAS POLÍTICAS?**

   _____
   _____

8. **LOS ENCARGADOS DE REDACTAR LAS POLÍTICAS FUERON:**
   - ○ a) Personal externo a la empresa
   - ○ b) Personal interno de la empresa
   - ○ d) OTROS:_____

9. **¿CÓMO DAN A CONOCER LAS POLÍTICAS EN LA EMPRESA?**
   - ☐ a) Vía correo electrónico
   - ☐ b) Mediante reuniones generales
   - ☐ c) Distribuidas físicamente a cada persona
   - ☐ d) OTROS:_____

10. **¿CADA CUÁNTO TIEMPO LA EMPRESA RENUEVA SUS POLÍTICAS?**
    - ○ a) Cada año
    - ○ b) Cada 2 años
    - ○ c) Cada 3 años
    - ○ d) OTROS:_____

11. **EN LA IMPLEMENTACIÓN DE CONTRASEÑAS, ¿QUÉ CONSIDERACIONES Y MÉTODOS MANEJAN?**
    - ☐ a) Exigencia en el formato de contraseña (límite en la longitud, usos de caracteres especiales, evitar palabras de diccionario, etc.)
    - ☐ b) Renovación de contraseña cada cierto tiempo
    - ☐ c) Utilización de software para administración de contraseña (generación, renovación, almacenamiento, eliminación, verificación)
    - ☐ d) OTROS:_____

12. **SEGÚN LA SIGUIENTE CLASIFICACIÓN, LA EMPRESA MANEJA INFORMACIÓN:**
    - ☐ a) Secreta
    - ☐ b) Confidencial
    - ☐ c) Uso interno solamente
    - ☐ d) Pública

13. **TIENEN IMPLEMENTADO CONTROLES DE SEGURIDAD PARA EL CUIDADO DE:**
    - ☐ a) La identificación del personal
    - ☐ b) Los bienes de la empresa
    - ☐ c) La información que maneja la empresa
    - ☐ d) El área de trabajo
    - ☐ e) OTROS:_____

14. **¿IMPLEMENTAN MEDIDAS SOBRE EL USO DE LA INFORMACIÓN INTERNA DE LA EMPRESA?**
    - ☐ a) Firmas de documentos legales bajo la responsabilidad del usuario, en caso de pérdida o plagio
    - ☐ b) Controles para la entrega, envío, seguimiento y devolución de la información
    - ☐ c) Control sobre la realización de copias, almacenamiento y eliminación de la información
    - ☐ d) OTROS:_____

15. **¿SE LIMITAN A CIERTOS DEPARTAMENTOS EL USO O ACCESO AL INTERNET?**
    - ○ a) Sí. Cuales:_____
    - ○ b) No

16. **¿LA EMPRESA OTORGA A LOS USUARIOS UN CORREO EXCLUSIVO PARA EL USO LABORAL?**
    - ○ a) Sí
    - ○ b) No

17. **¿SE LE PERMITE A LOS USUARIOS REALIZAR OPERACIONES DE TRABAJO UTILIZANDO UN CORREO DIFERENTE AL OTORGADO POR LA EMPRESA?**
    - ○ a) Sí
    - ○ b) No

18. **¿LA EMPRESA POSEE SISTEMAS MULTIUSUARIOS?**
    - ○ a) Sí
    - ○ b) No (Pase a la 20)

19. **¿CUÁL DE LOS SIGUIENTES CONTROLES DE SEGURIDAD, SON IMPLEMENTADOS EN SU EMPRESA PARA LA PROTECCIÓN DE LOS SISTEMAS MULTIUSUARIOS?**
    - ☐ a) Identificadores únicos de usuario y contraseña
    - ☐ b) Clasificación de usuarios en base a privilegios
    - ☐ c) Firma de declaración de conformidad
    - ☐ d) OTROS:_____

20. ¿LA EMPRESA CUENTA CON ALGÚN TIPO DE SEGURO QUE CUBRA LA INTEGRIDAD DE LA INFORMACIÓN Y LA DEL PERSONAL?

- ○ a) Sí
- ○ b) No

OBSERVACIONES Y/O COMENTARIOS: _____

_____

_____

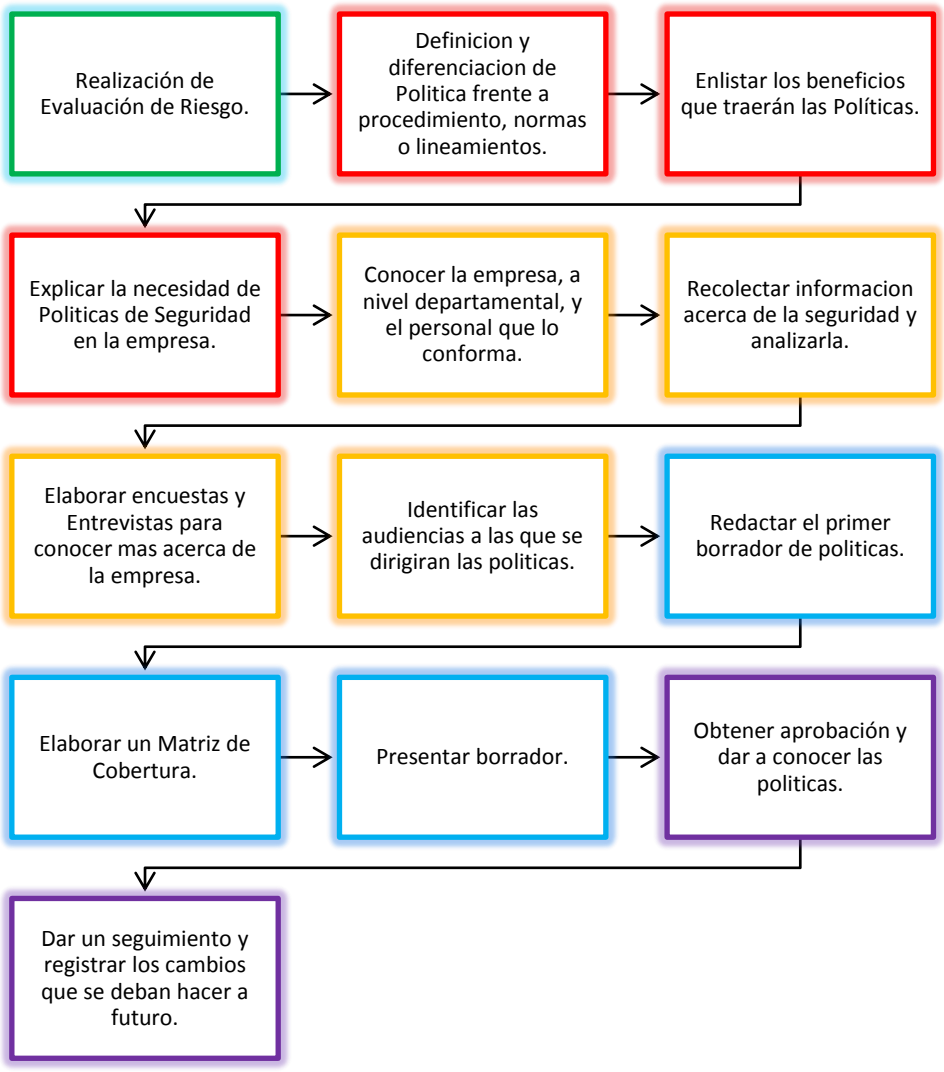
_____

_____

_____

ANEXO D

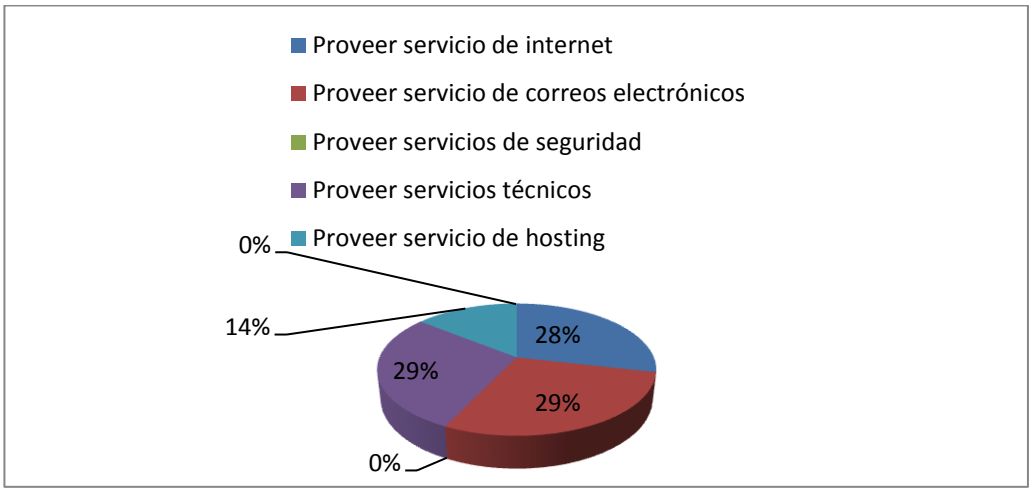
DIAGRAMA DE FLUJO DE LOS PASOS QUE SE DEBEN SEGUIR PARA EL DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD.



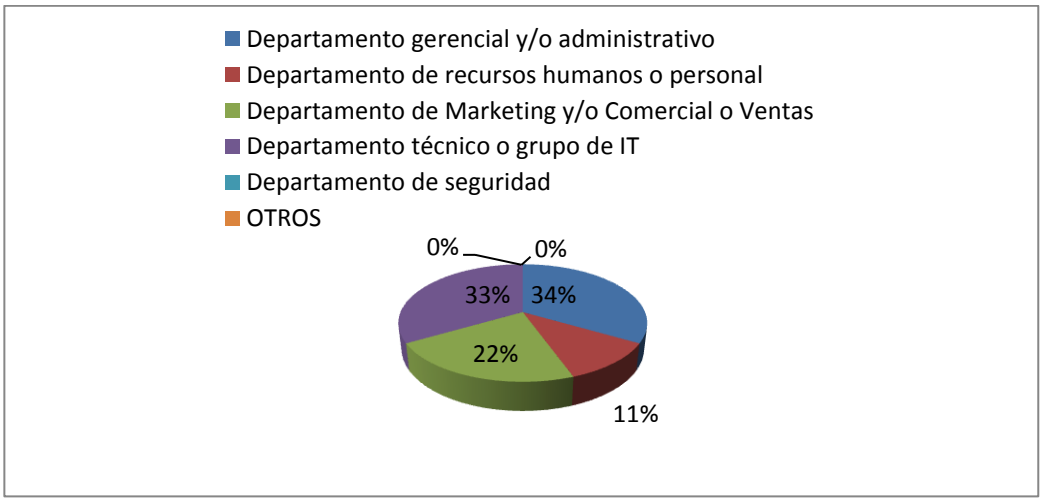
ANEXO E

DIAGRAMAS QUE MUESTRAN EN PORCENTAJE LAS RESPUESTAS DE LAS EMPRESAS SEGÚN LA ENCUESTA DEL ANEXO C.

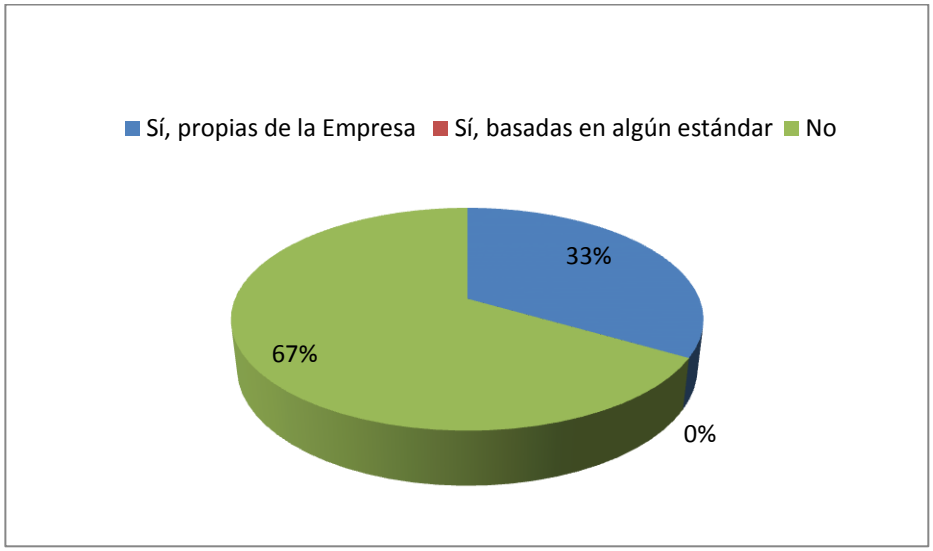
1. ¿A QUÉ SE DEDICA LA EMPRESA?



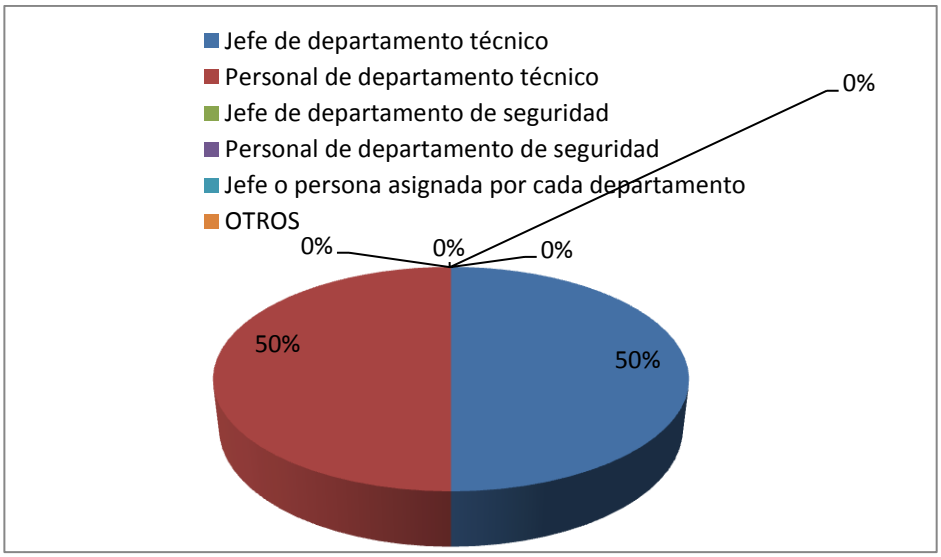
2. INDIQUE LOS DEPARTAMENTOS QUE POSEE LA EMPRESA



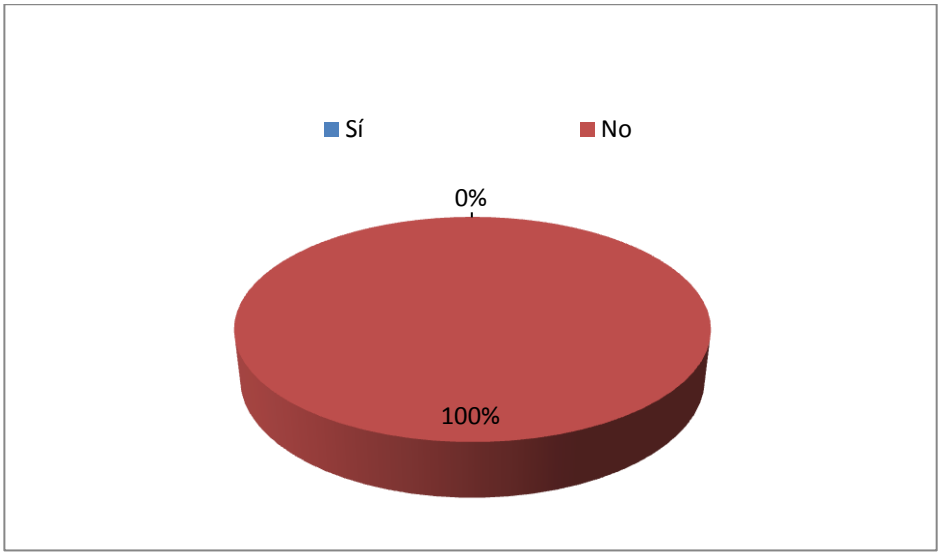
3. **¿LA EMPRESA POSEE O SE BASA EN ALGÚN TIPO DE POLÍTICAS DE SEGURIDAD ESTANDAR?**



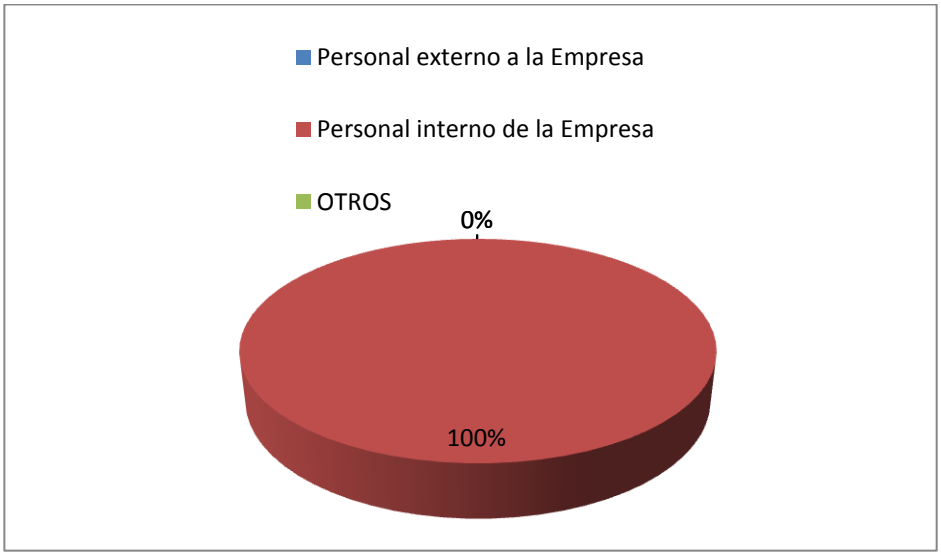
4. **¿QUIÉN ES EL ENCARGADO DE CONTROLAR EL CUMPLIMIENTO DE SUS POLÍTICAS?**



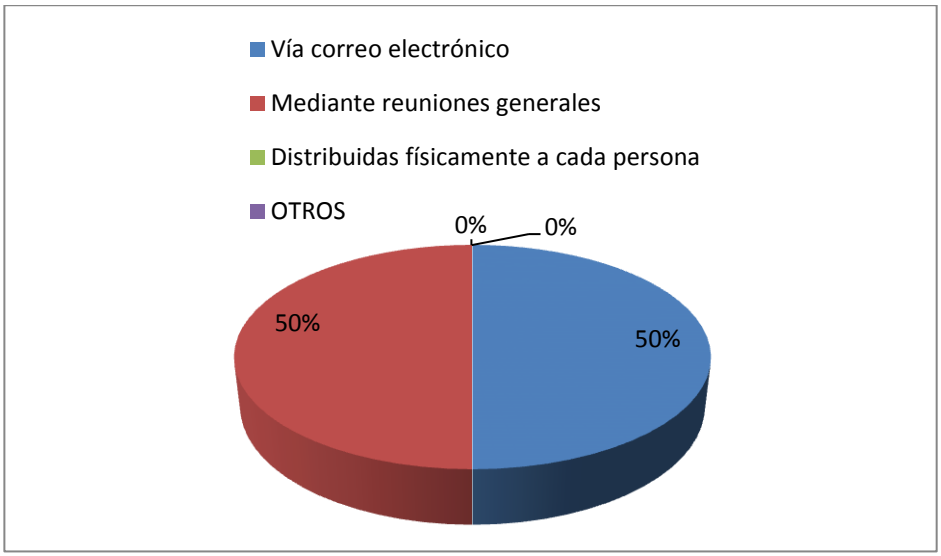
5. ¿HAN TENIDO ALGÚN PROBLEMA CON EL CUMPLIMIENTO DE LAS POLÍTICAS?



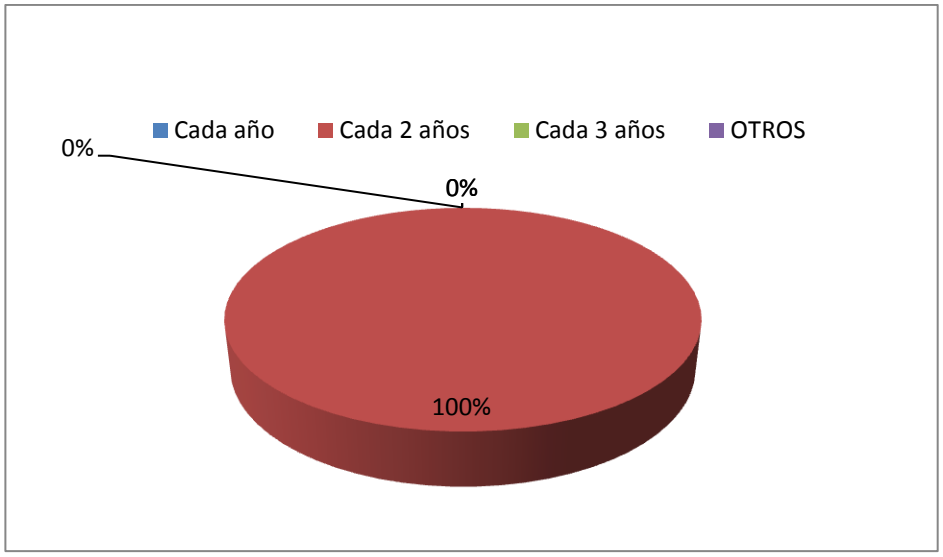
8. LOS ENCARGADOS DE REDACTAR LAS POLÍTICAS FUERON:



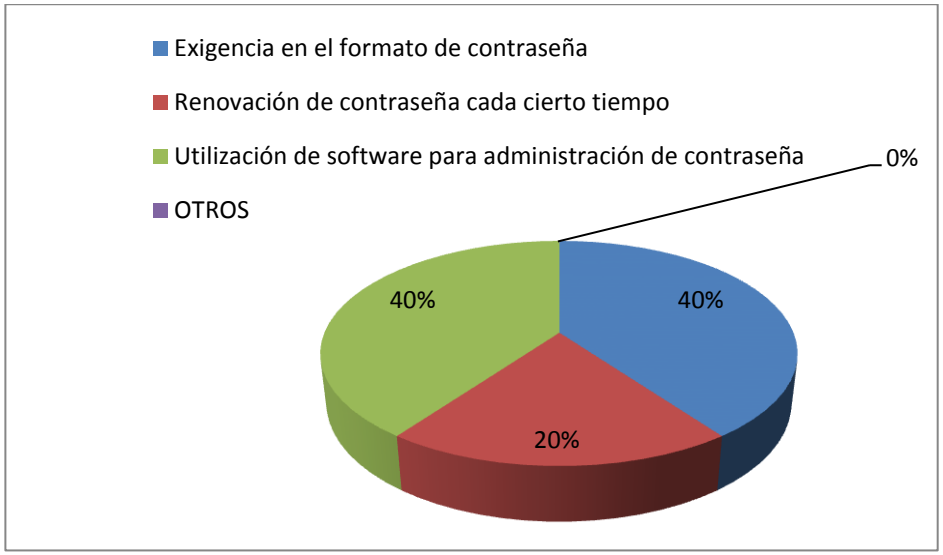
9. ¿CÓMO DAN A CONOCER LAS POLÍTICAS EN LA EMPRESA?



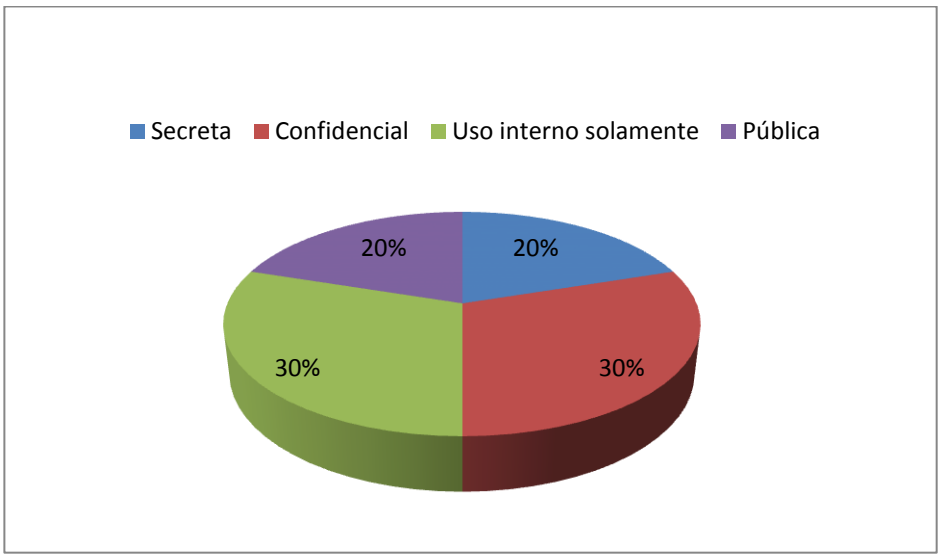
10. ¿CADA CUÁNTO TIEMPO LA EMPRESA RENUEVA SUS POLÍTICAS?



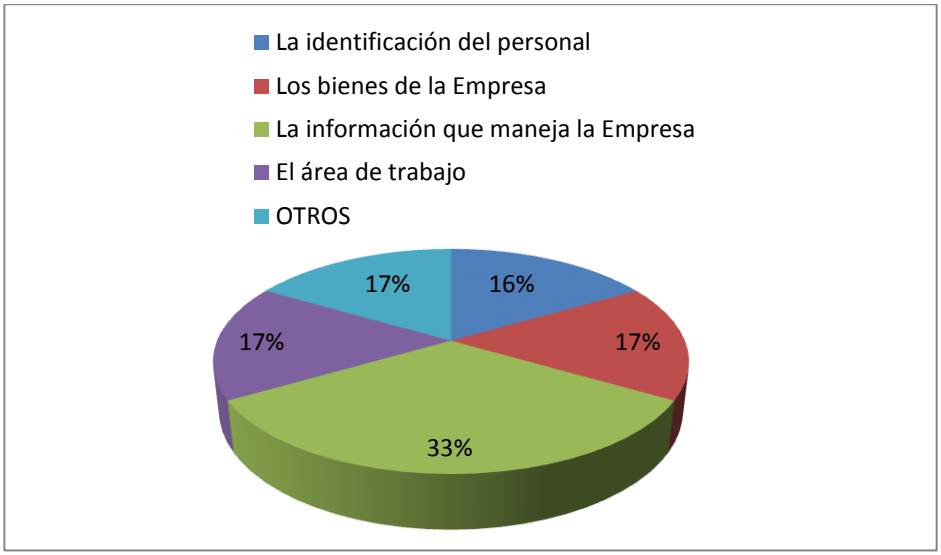
11. EN LA IMPLEMENTACIÓN DE CONTRASEÑAS, ¿QUÉ CONSIDERACIONES Y MÉTODOS MANEJAN?



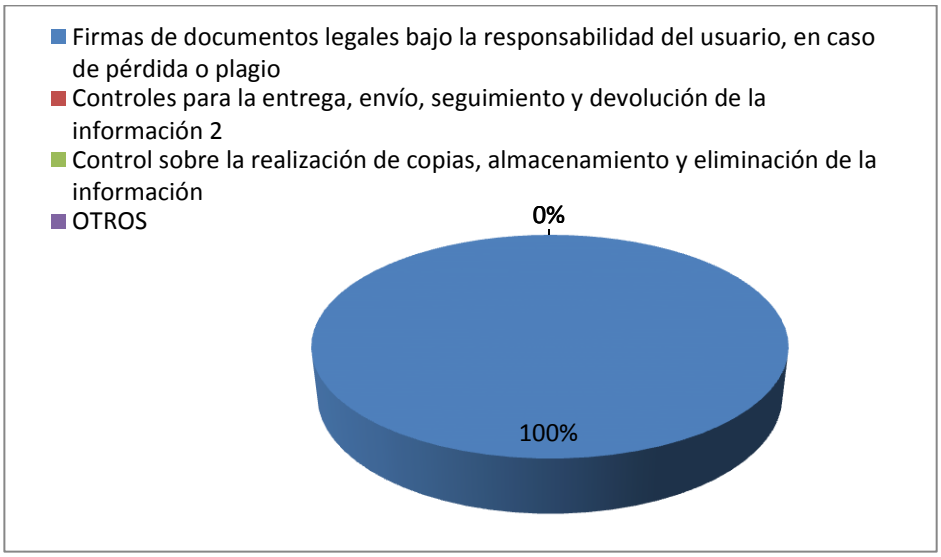
12. SEGÚN LA SIGUIENTE CLASIFICACIÓN, LA EMPRESA MANEJA INFORMACIÓN



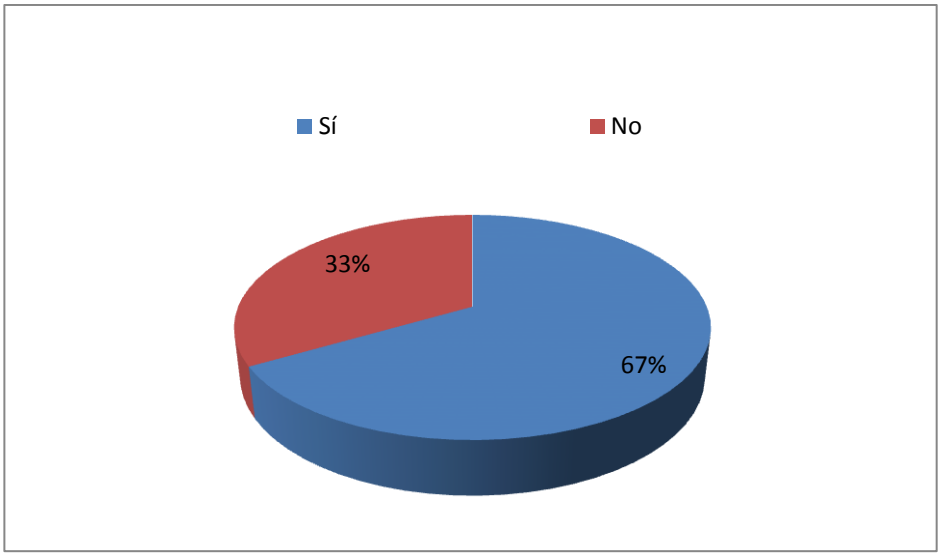
13. TIENEN IMPLEMENTADO CONTROLES DE SEGURIDAD PARA EL CUIDADO DE:



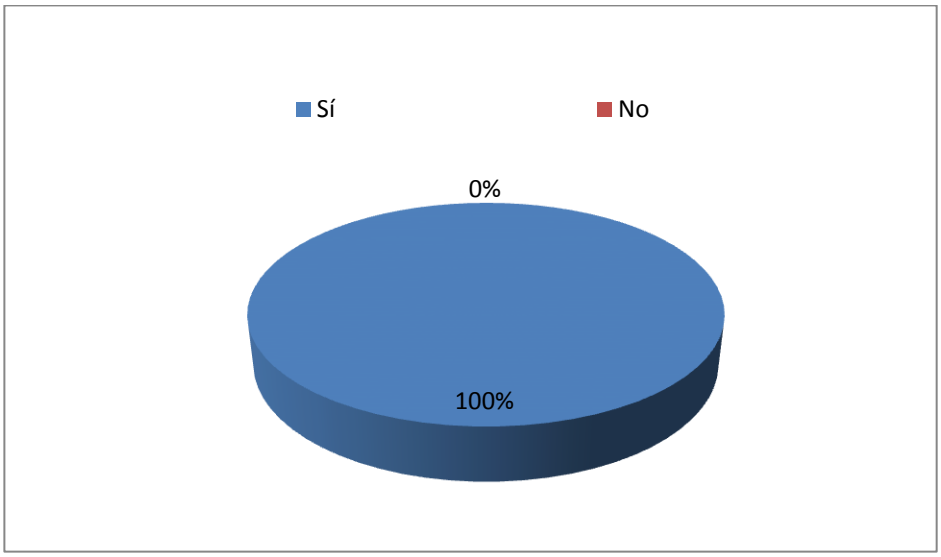
14. ¿IMPLEMENTAN MEDIDAS SOBRE EL USO DE LA INFORMACIÓN INTERNA DE LA EMPRESA?



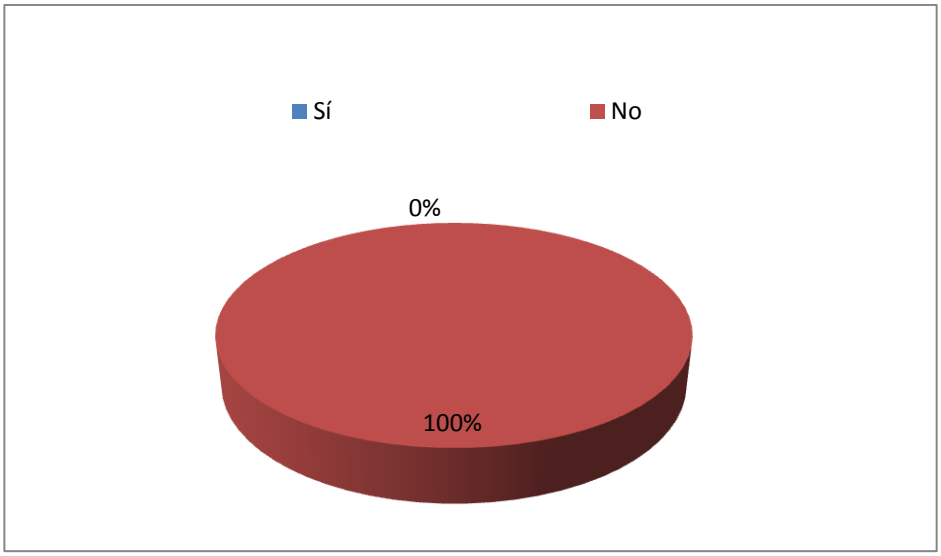
15. **¿SE LIMITAN A CIERTOS DEPARTAMENTOS EL USO O ACCESO AL INTERNET?**



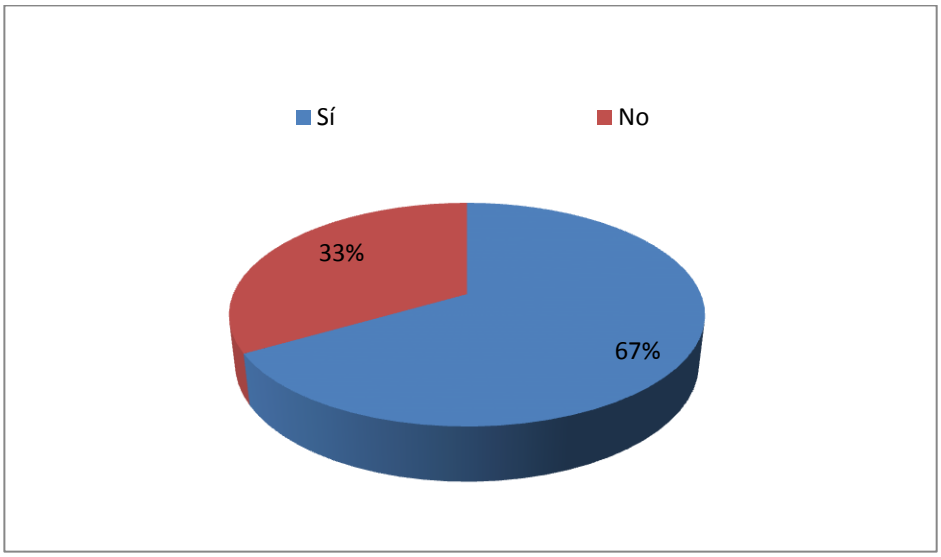
16. **¿LA EMPRESA OTORGA A LOS USUARIOS UN CORREO EXCLUSIVO PARA EL USO LABORAL?**



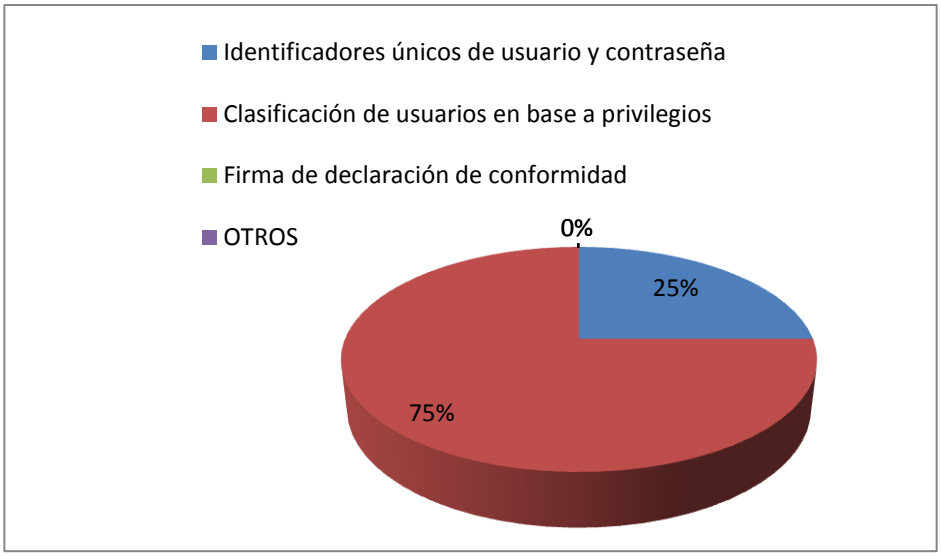
17. ¿SE LE PERMITE A LOS USUARIOS REALIZAR OPERACIONES DE TRABAJO UTILIZANDO UN CORREO DIFERENTE AL OTORGADO POR LA EMPRESA?



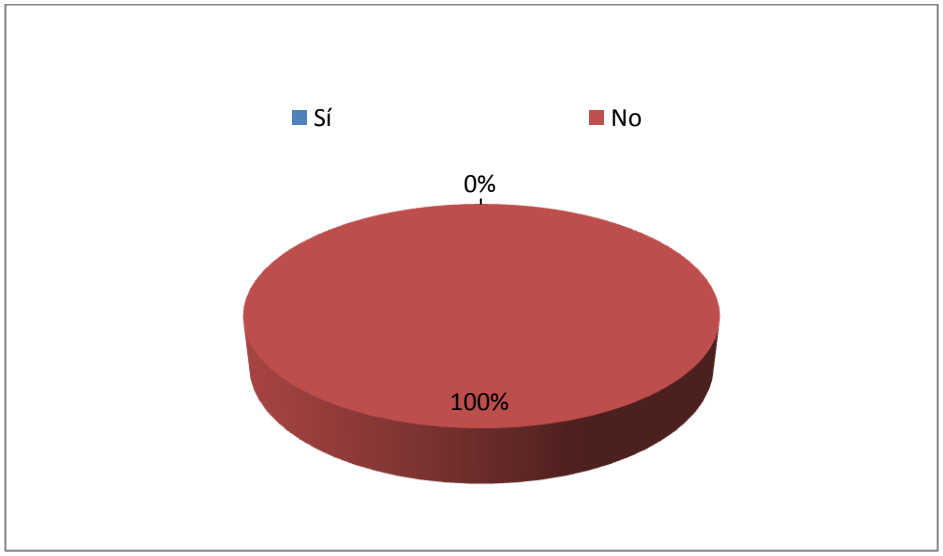
18. ¿LA EMPRESA POSEE SISTEMAS MULTIUSUARIOS?



19. ¿CUÁL DE LOS SIGUIENTES CONTROLES DE SEGURIDAD, SON IMPLEMENTADOS EN SU EMPRESA PARA LA PROTECCIÓN DE LOS SISTEMAS MULTIUSUARIOS?



20. ¿LA EMPRESA CUENTA CON ALGÚN TIPO DE SEGURO QUE CUBRA LA INTEGRIDAD DE LA INFORMACIÓN Y LA DEL PERSONAL?



ANEXO F

MATRIZ DE CRITICIDAD VS PROBABILIDAD

Criticidad / Probabilidad	ALTA	MEDIA	BAJA
ALTA	25	15	5
MEDIA	15	9	3
BAJA	5	3	1

REFERENCIAS

[1] Charles Cresson Wood, CISA, CISSP. Políticas de Seguridad Informática – Mejores Prácticas Internacionales, Conjunto Complejo de Políticas de Seguridad Informática, Versión 9. Publicado por NetIQ, Inc, Septiembre 2002, pág. 6

[2] Subsecretaría de Tecnologías Informáticas – Secretaría de la Función Pública. Manual de Seguridad en Redes, Coordinación de Emergencia en Redes Teleinformática. http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf. Consultado el 14 de Enero del 2011, pág. 1-1

[3] Antonio Villalón Huerta, El Sistema de Gestión de Seguridad de la Información, "La Nueva Norma UNE 71502". Grupo S2, Septiembre 2004. http://www.shutdown.es/ISO17799.pdf. Consultado el 16 de Enero del 2011.

[4] Microsoft-TechNet**,** Guía de administración de riesgos de seguridad de Microsoft. Octubre 2004. http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx . Consultado el 20 de Enero del 2011.

[5] Organización Internacional para la Estandarización, Abstracto del ISO/IEC 27000:2009. Junio 2010. http://www.iso.org/iso/catalogue_detail?csnumber=41933. Consultado el 16 de Enero del 2011.

[6] Scott Barman, “Writing Information Security Policies”, Publishing by New Riders, First Edition, November 2001.