LA SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN (TI) COMO UNA VARIABLE DE LA CULTURA ORGANIZACIONAL

VICTOR MANUEL BAENA CANO

Universidad EAFIT

Escuela de Administración y Negocios

2009

LA SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN (TI) COMO UNA VARIABLE DE LA CULTURA ORGANIZACIONAL

VICTOR MANUEL BAENA CANO

Asesor

Mg. Luis Giovanni Restrepo Orrego

UNIVERSIDAD EAFIT

MAESTRIA EN ADMINISTRACION

ESCUELA DE ADMINISTRACIÓN Y NEGOCIOS

MEDELLIN

2009

Nota de Aceptación

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Medellín, 30 de Noviembre de 2009

CONTENIDO

INTRODUCCIÓN *16*
1. ESTADO DEL ARTE *20*
1.1. CONCEPTO CULTURA: 21
1.2. LA CULTURA Y EL HOMBRE 22
1.3. CULTURA ORGANIZACIONAL 32
1.3.1. El clima organizacional 39
1.4. Seguridad de Tecnología Informática (TI) 45
2. MARCO TEÓRICO *54*
2.1. SEGURIDAD DE TECNOLOGÍA: CRITERIOS GENERALES, CONCEPTOS Y PREMISAS: 54
2.2. LA CULTURA DE SEGURIDAD DE TECNOLOGIA DE INFORMACIÓN (TI) 63
2.2.1. Convergencia de la seguridad: 67
2.2.2. Consecuencias de la seguridad en la organización: 68
2.2.3. Compromiso organización en la seguridad: 68
2.2.4. Plan de seguridad de la información: 70
2.2.5. Elaboración de una política de seguridad: 70
2.2.6. Creación de una estructura de gestión de la seguridad: 70
2.2.7. Establecimiento de los procedimientos de seguridad: 71
2.2.8. Distribución de los procedimientos de seguridad: 71
2.2.9. Éxito del plan de seguridad: 71
2.3. ¿CÓMO DEBEMOS DEFINIR EL CONTROL? 72
2.3.1. ¿Qué papel juega el control en los sistemas de información? 73
2.4. FUNDAMENTOS DE UN MODELO DE SEGURIDAD INFORMÁTICA 75
2.4.1. Lecciones del libro naranja 76

2.4.2. Information Technology Segurity Evaluation Criteria (ITSEC) 80
2.4.3. Lista de preocupaciones 83
2.4.4. Análisis de riesgos 92
2.5. MODELO DE SEGURIDAD DE TECNOLOGÍA DE INFORMACION (TI).... 110
2.5.1. Misión de seguridad 111
2.5.2. Consenso 113
2.5.3. El método Delphi 114
2.5.4. Políticas de seguridad 119
2.6. ENCUESTA 120
2.6.1. Modelo de encuesta 120
2.6.2. Tabulación y síntesis argumentativa del instrumento estadístico 127
2.6.3. Etapas para desarrollar un modelo de seguridad de TI 152
CONCLUSIONES 155
BIBLIOGRAFIA 156
ANEXO 1 167
ANEXO 2 172
ANEXO 3 188

TABLAS

Tabla 1. Niveles -Libro Naranja- 77
Tabla 2. Clasificación en Niveles -Libro Naranja- 77
Tabla 3. Conceptos de políticas y clasificación de la información..... 78
Tabla 4. Concepto de responsabilización 78
Tabla 5. Concepto de documentación como elemento de seguridad 79
Tabla 6. Conceptos de garantías requeridas 79
Tabla 7. Correspondencia entre el *"Orange Book" y "White Book"* 83
Tabla 8. Tabla para dar prioridades a las amenazas 104
Tabla 9. Hoja de factor de riesgo 104
Tabla 10. Controles del CSI/FBI 106
Tabla 11. ¿Cuál es el sector primario de su empresa?..... 128
Tabla 12. ¿Cuántos empleados tiene su organización? 129
Tabla 13. ¿Cuál es su cargo en la organización? 130
Tabla 14. ¿Cuál es área en la que se desempeña? 132
Tabla 15. ¿Qué tan frecuentemente usa Internet para su trabajo?..... 133
Tabla 16. ¿Tiene la empresa en la cual trabaja una estrategia de seguridad de TI? 134
Tabla 17. ¿Qué tan importante es la seguridad de TI para su empresa? 135
Tabla 18. ¿Está su empresa capacitando a su personal para afrontar los problemas de seguridad de TI? 136
Tabla 19. ¿Cuál es el medio por el cual su empresa capacita a los empleados en la seguridad de TI? 137

Tabla 20. ¿Conoce usted las reglas, normas y políticas de la empresa en seguridad de TI? 138
Tabla 21. ¿Cree usted que las reglas, normas y políticas de la empresa en seguridad de TI son consecuentes con su actuar personal? 139
Tabla 22. ¿El proceso de comunicación utilizado en la empresa sobre la seguridad de TI considera que es? 140
Tabla 23. ¿Cree usted que sus logros personales sobre el conocimiento de la seguridad de TI se están cumpliendo en la empresa? 141
Tabla 24. ¿Se considera usted parte importante en la de seguridad de TI de su empresa? 141
Tabla 25. ¿Si hay un incidente de seguridad de TI en su empresa usted lo reporta al área encargada? 142
Tabla 26. ¿Cuál es el área encargada de manejar la seguridad de TI de su empresa? 143
Tabla 27. ¿En su empresa lo han tenido en cuenta para el desarrollo de la estrategia de la seguridad de TI? 144
Tabla 28. ¿Es usted consciente y conoce los riesgos y las medidas preventivas correspondientes a cumplir con la seguridad de TI? 145
Tabla 29. ¿Ha sido difícil el cambio de su trabajo convencional al trabajo cumpliendo los parámetros de la seguridad de TI? 146
Tabla 30. ¿En su empresa le hacen monitoreo y seguimiento al manejo de la información de la organización? 147
Tabla 31. ¿Considera que el tema de seguridad de TI, es algo muy complejo, difícil de aprender y un duro de asimilar? 147
Tabla 32. Su empresa es al día de hoy en el manejo de la información basada en las políticas de seguridad de TI 148
Tabla 33. Sus compañeros de trabajo opinan sobre seguridad de TI que es para la organización 149
Tabla 34. ¿Ha tenido usted incidentes de seguridad de TI? 150

Tabla 35. ¿El personal directivo de su empresa los incentiva y los apoya en el proceso de seguridad de TI? 150
Tabla 36. ¿Existe un verdadero compromiso de su empresa en la seguridad de TI? 151

GRÁFICOS

Gráfico 1. Cuadro de clasificación de amenazas.....93

GLOSARIO

Activo informático: puede ser datos, información, sistema, software, hardware, o cualquier elemento de tecnología de información.

Amenaza: Un evento con el potencial de causar un acceso no autorizado, modificación, revelación o destrucción de información, aplicaciones, sistemas, servicios o procesos. Una acción o acción potencial con posibilidad de causar daño.

***Backdoor*:** Puerta trasera de un sistema informático, un mecanismo del software que permite entrar evitando el método usual. Son fallas en el diseño del sistema.

Bien: Algo con valor para la institución que necesita ser protegido.

Bombas Lógicas: Programa que se activará en un momento determinado llenando la memoria de la computadora. Programa orientado a colapsar el sistema de correo electrónico, este se suele llamar *mailbombing*.

Boxes: Aparatos electrónicos o eléctricos cuya finalidad es el phreaking, emula la introducción de monedas en teléfonos públicos. Las más conocidas son la *bluebox*, la *redbox* y la *blackbox*.

***Bug, Hole*, Agujero:** Se trata de un defecto en el software, generalmente en el sistema operativo que permite la intrusión de los hackers.

Caballos de Troya: Programas que simulan ser otros para así atacar el sistema. Programas que se queda residente en un sistema informático y facilita información sobre lo que ocurre en el mismo (*passwords*, *logins*, etc.). También es aplicable a programas que parecen normales y que al ejecutarse despiertan un virus que se introduce en el sistema. El troyano más famoso es sin duda el *BackOrifice*, un troyano que utiliza las puertas traseras, apareció el 8 de agosto de 1998. Incluso aparece la versión para linux desarrollada por CDC (*Cult of the death cow*. Culto a la vaca muerta).

***Carding*:** Uso fraudulento de tarjetas de crédito o sus números. Ello incluye la generación de nuevas tarjetas de crédito.

Confidencialidad: La información sólo puede ser conocida por individuos autorizados.

Código Malicioso ("*malware*"): Es cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático. Están incluidos los virus, troyanos, gusanos, bombas lógicas, etc.

Control, salvaguarda o mecanismo: Medida de protección (técnica o normativa) de los activos informáticos.

Cortafuego, *firewall*, bastión: Software y/o Hardware de seguridad encargado de chequear y bloquear el tráfico de la red hacia un sistema determinado.

Crackeador o *crack*: Son programas que se utilizan para desproteger o sacar los *passwords* encriptadas de programas comerciales, pudiéndose utilizar éstos como

si se hubiera comprado la licencia. Quienes los distribuyen son altamente perseguidos por las actividades que protegen los productos de software.

***Cracker*:** Un individuo que se dedica a eliminar las protecciones lógicas y físicas del software, normalmente muy ligado al pirata informático, puede ser un *hacker* criminal o un *hacker* que daña el sistema en el que intenta penetrar

Disponibilidad: Seguridad de que la información pueda ser recuperada en el momento que se necesite.

El gran hermano: En el mundo del *hacking* se conoce por este término a cualquier empresa poderosa que intenta controlar el mercado y el mundo de la informática. En este estado podríamos colocar a la IBM, Microsoft, empresas telefónicas, etc.

***Exploit*:** Método de utilizar un *bug* para penetrar en un sistema.

Fuerza Bruta: Forma poco sutil de entrar en un sistema y consiste en probar distintas contraseñas hasta encontrar la adecuada. Requiere mucho tiempo y para ello se emplea un crackeador que desencripta un archivo y obtiene las claves del archivo de *passwords* empleando las palabras del diccionario, etc.

Gusanos: También conocidos como *worms*. Programas que se copia a si mismo llegando a crear miles de replicas del mismo y destruyendo la información del sistema.

***Hacking*:** Entrar en forma ilegal y sin el consentimiento del propietario en su sistema informático. No conlleva a la destrucción de datos ni a la instalación de

virus. También lo podríamos definir como cualquier acción encaminada a conseguir la intrusión en un sistema (ingeniería social, caballos de trolla, etc.)

Impacto: Aquellas pérdidas producto de la actividad de las amenazas. Estas pueden manifestarse como destrucción, interrupción, modificación y exposición de los bienes de la institución.

Ingeniería social: Es una técnica por la cual se convence a alguien por diversos medios para que proporcione información útil para *hackear* o para beneficiarnos. Requiere grandes dosis de psicología y explota la tendencia de la gente a confiar en sus semejantes.

Integridad: Garantía que la información no ha sido alterada, borrada, copiada, etcétera.

***Lamer*:** Principiante en el mundo del *hacking*, que se las da de listo o que copia descaradamente el trabajo de otros *hackers*. Cuando se les descubre se les desprecia y se les expulsa del círculo en el que se ha introducido.

***Phreakers* (crackers telefónicos):** Distinguidos por que utilizan líneas telefónicas para sus actos. Este término mezcla las palabras inglesas *phone* (teléfono) y *freak* (monstruo o 'bicho raro'). *Phreaking*. Acciones tendientes a utilizar fraudulentamente las líneas telefónicas, es decir, todo lo relacionado con el uso del teléfono o servicios telefónicos de forma gratuita; también incluye la modificación o intervención de las líneas telefónicas y modificaciones de aparatos telefónicos con el fin de comunicarse gratuitamente.

Pirata informático: Es un delincuente informático que se dedica a la copia y distribución de software ilegal. Este software puede ser comercial craqueado o

shareware registrado. También es otro nombre que reciben los crackers, no confundir con los hackers.

Plan de seguridad: Es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.

Política de seguridad: “Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran” (RFCs 1244 y 2196)

Procedimiento de seguridad: Es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implementar las políticas de seguridad que han sido aprobadas por la organización.

Proceso crítico: Todo proceso que impacte directamente en la consecución de los objetivos de la organización.

Riesgo residual: Riesgo que permanece después de aplicar medidas de mitigación a un riesgo.

Riesgo: El riesgo puede ser definido como "algo que puede causar un daño", o como lo define. La probabilidad de que un evento adverso ocurra contra un bien.

Seguridad de TI: Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o

integridad, disminuir el rendimiento de los equipos o bloquear el acceso a de usuarios autorizados al sistema.

Sistemas de información: Un sistema de información (SI) es un conjunto de datos organizados listos y preparados para su posterior uso, generados por una necesidad: Personas, datos, actividades o técnicas de trabajo, Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente). Todo interactúa entre sí para procesar los datos y la información (incluyendo procesos manuales y automáticos) y distribuirla de la manera más adecuada posible en una determinada organización en función de sus objetivos.

***Sniffer* y *Sniffing*:** Un *sniffer* es un programa que intercepta la información que transita por una red. *Sniffing* es espiar y obtener la información que circula por la red, su misión es fisgonear la red en busca de claves o puertos abiertos.

***Snoop*:** Fisgonear, mirón. Persona que está pendiente de los que pasa en la red y esperando encontrar información importante o huecos de seguridad.

***Spams*:** No es un código dañino, pero sí bastante molesto; es un programa que ejecuta una orden repetidas veces. Ampliamente utilizado por empresas de marketing, usando el correo electrónico para enviar sus mensajes en forma exagerada.

Tracear: Seguir a través de la red, la pista de una información o una persona. Se utiliza por las grandes empresas como las telefónicas, para obtener la identidad de los sospechosos o *hackers*.

Trashing**:** Recoger basura. Se trata de buscar en la basura (física o informática), información que pueda ser útil para *hackear*.

Virus Informático: Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos por que no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (*payload*) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Vulnerabilidad: Condición de debilidad. Al no existir vulnerabilidades, las amenazas no tendrían impacto alguno en la institución. Debilidad, defecto o falla

War Dialer **(Discador):.** Programa que escanea las líneas de teléfonos en búsqueda de *modems*.

RESUMEN

Ésta investigación pretende abordar de forma global, la seguridad de tecnología de información y cómo se articula ésta con la cultura organizacional, para llegar a demostrar que la seguridad de TI es una variable de la cultura de la organización o denominada también como "cultura de seguridad de TI". Se analizan los componentes que permiten definir el concepto de cultura hasta su contextualización en el marco de las teorías administrativas y de la organización, escenario en el cual se desarrolló una prueba empírica para el análisis de la problemática de la seguridad de TI que se presenta en las organizaciones, cuando sólo se tienen en cuenta los aspectos técnicos y se demerita el valor que posee el factor humano.

Este texto, se ha estructurado bajo dos grandes componentes temáticos: se abordan inicialmente los referentes teóricos de cultura, cultura organizacional y seguridad de TI para articularlos conceptualmente con el desarrollo de la investigación y de un modelo de seguridad de TI en la cual se corroboran las hipótesis de trabajo.

Palabras clave: cultura, cultura organizacional, seguridad de tecnología, cultura de seguridad de TI y modelos de seguridad de TI.

ABSTRACT

This research aims to address in a global form, the information of technological security and how it articulates with the organizational culture, to prove that IT security is a variable of the culture of the organization or also known as "safety culture IT ". It discusses the components that define the concept of culture to its contextualization in the context of administrative theories and the organizational setting in which an empirical test was developed to analyze the problems of IT security that occurs in organizations, when only taking into account the technical and diminishes the value of the human factor.

This text is structured under two main thematic components: initially addressed are the theoretical references of culture, organizational culture and IT security to articulate conceptually to the research and development of an IT security model in which the working hypothesis can be corroborated.

Keywords: Culture, organizational culture, security of technology, IT security culture and models of IT security.

INTRODUCCIÓN

El presente trabajo abarca el tema de la seguridad de tecnología de información (TI) en las organizaciones como una estrategia que implica la implementación de políticas, procedimientos e infraestructura tecnológica y cómo esa seguridad de tecnología puede convertirse en una variable de la cultura de la organización.

Para su desarrollo, comenzamos por analizar la actualidad de la seguridad de tecnología en algunas empresas, esto es, en empresas de servicios financieros, manufactureras, de consultoría, de ventas, seguros, entre otras para visualizar y evaluar cómo ha sido al interior de las mismas su evolución, asimismo, cómo ven este aspecto los usuarios y las directivas empresariales. En este orden de ideas, la forma como puede llagar a ser la seguridad de tecnología una variable de la cultura organizacional.

Con el trabajo de investigación conceptual, teórica, la aplicación y diseño de un instrumento estadístico, logramos obtener resultados que nos permitieron ponderar aspectos como la percepción de la seguridad de TI en todo el personal de las empresas, desde los directivos hasta los usuarios comunes, los procesos que se desarrollaron o se desarrollarán para que la seguridad de tecnología sea una variable en la cultura de la organización y, adicionalmente, para proveer y generar criterios que puedan llegar a cuantificar en la organización la evolución que ha tenido o tiene la seguridad de TI y la apropiación de cada uno de los miembros de la organización en este aspecto. Lo anterior ha generado que en las empresas se están creando áreas especializadas en el manejo de la seguridad de

la información ó conocidas como seguridad de TI (tecnología de la información), siendo las encargadas en la implementación de procesos, políticas y toda la infraestructura tecnológica con herramientas que ayudan a proteger la información. Cada una de las tareas que desarrolla el área de seguridad de TI contribuyen a incrementar la seguridad de la información, por ejemplo, con las políticas se definen los reglamentos y normas de comportamiento con la información de la compañía, con los procesos se definen los procedimientos para el manejo de la información y con los equipos especializados, se detectan posibles violaciones, virus o intentos de robo o alteración de la información.

Ahora, con la información anterior se contextualizó la problemática e hipótesis de estudio para proponer un modelo teórico que involucra la organización en la era de la seguridad de tecnología información (TI), toda vez que es un tema que compete a la organización en su conjunto, es decir, desde los empleados de menor rango o jerarquía en la empresa hasta los directivos de la misma, con el apoyo de las áreas de tecnología encargadas del manejo, implementación, administración y otras áreas como contraloría para el control, definición de políticas, normas, etc. y en general, toda la organización para tener un marco global sobre la información que maneja la empresa.

Los problemas de seguridad de TI no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a la de su punto más débil. Por mucha tecnología de seguridad que se implante en una organización, si no existe una clara disposición por parte de la dirección general y una cultura a un nivel de usuarios, no se conseguirán los objetivos perseguidos con la implementación de un sistema de seguridad. La importancia de esta investigación puede argumentarse en los beneficios que para las empresas traerán sus resultados, toda vez que estamos seguros servirá para diseñar desde el área de seguridad políticas, estrategias, metodologías de control y se afiance el conocimiento de ésta

en la consolidación de una cultura de seguridad de TI en todos los empleados. En este escenario, el alcance dado a esta investigación busca fundamentalmente identificar cómo las implementaciones que se llevan a cabo por el área de seguridad de TI de las empresas, se constituyen en una variable en la cultura de la organización y llegan a identificar otras variables para poder evaluar cómo se ha influenciado el ethos de la organización con la implementación de los procesos, evaluación, estrategias, políticas e infraestructura de seguridad en la empresa.

Logramos proponer y desarrollar un modelo de seguridad con sus respectivas estrategias y demás componentes para lograr que la seguridad de TI se convierta en una variable más en la cultura de la organización, o sea, lograr que los empleados tengan un nivel el conocimiento y la conciencia necesaria en el tema de seguridad de TI tal que para cada uno de ellos la maneje y apropie como algo natural y cotidiano el manejo del mismo.

La metodología desarrollada en el proceso de investigación se estructuró teniendo en cuenta que el tipo de estudio propuesto fue el de una investigación exploratoria, no experimental, es decir, teórico. La investigación se desarrolló mediante la profundización de los componentes temáticos de la cultura organizacional y sobre la seguridad de TI, que fueron analizados por separado y luego se argumentan como resultado de la investigación articulando la seguridad de TI como variable constitutiva de la cultura organizacional.

Para ello, se realizó el análisis de la información recolectada para lograr interrelacionar éstas temáticas y diseñar así un modelo con sus respectivas políticas, estrategias, tecnología, etc., para que la seguridad se convierta en una variable de la cultura organizacional. En consecuencia, el presente trabajo se estructuró expositivamente en dos grandes componentes temáticos: La cultura, sus conceptualizaciones, la cultura organizacional y los componentes de la

seguridad de TI y, por último la propuesta de un modelo que articula en la práctica nuestra temática de investigación., con el instrumento estadístico y la tabulación de la información recogida; terminando con el apartado de las conclusiones resultantes de la formación como Mg. en Administración de Empresas y el aprendizaje alcanzado con el desarrollo de la investigación, en la cual, debo agradecer especialmente al Dr. Iván Darío Toro, por su paciencia, diligencia y ayuda en la valoración, definición tanto del proyecto como la evaluación general del trabajo de investigación; también debo agradecer al asesor del proyecto de investigación Mg. Luis Giovanni Restrepo Orrego, por el tiempo dedicado a acompañamiento y ayuda en el proceso de elaboración, revisión, recolección, redacción, análisis y elaboración del informe final de este trabajo de grado. Asimismo al cuerpo docente de la maestría y a todos aquellos que de una u otra forma me colaboraron y/o se vieron afectados por este proceso de formación académica e intelectual, que esperamos haber concluido satisfactoriamente.

.

1. ESTADO DEL ARTE

Alrededor de ambas temáticas existe un buen cúmulo de información, pero dispersa una de la otra y, en consecuencia, sin ningún tipo de articulación que evidencie que halla sido considerada de acuerdo al propósito que define nuestra investigación, en otras palabras, el presente trabajo abarca el tema de la seguridad de tecnología de información (TI) y en las organizaciones como una estrategia que implica la implementación de políticas, procedimientos e infraestructura tecnológica y cómo esa seguridad de tecnología puede convertirse en una variable de la cultura de la organización.

El investigador H. Abarbanel[1], afirma que sobre la cultura en las organizaciones es realmente mucho lo que se ha escrito y existen diversas y variadas propuestas teóricas sobre este particular, y se observan como temas que tienen un alto grado de madurez y una producción investigativa amplia. Con lo cual el propósito de la investigación no es únicamente el análisis de la cultura de la organización sino cómo se articula ésta con el de la seguridad de tecnología.

En resumen, la cultura de la organización ayuda a enfocar y contextualizar mejor la investigación. La palabra cultura se deriva metafóricamente de la idea de "cultivo", el proceso de cuidar y desarrollar la tierra. Así, pues, cuando hablamos de cultura nos estamos refiriendo a los modelos de desarrollo reflejados en un sistema de sociedad compuesto de conocimientos, ideologías, valores, leyes y un ritual diario. La palabra se utiliza frecuentemente para referirse al grado de

[1] ABARBANEL, H. Cultura organizacional, Aspectos Teóricos, prácticos y metodológicos. Bogotá: Ed. Legis, 2005. 489p

refinamiento evidente del tal sistema de creencias y prácticas. Ambos usos se derivan de las observaciones decimonónicas de las "sociedades primitivas", conviniendo en la idea que diferentes sociedades manifiestan diferentes niveles y patrones de desarrollo social. Hoy en día, sin embargo, el concepto de cultura no conlleva necesariamente esta anticuada postura, siendo más general el significado que diferentes grupos de personas tienen diferentes modos de vida. El Dr. Fernando Toro Álvarez[2], concluye que la cultura resulta ser un contexto general, multifacético y multidimensional que incide sobre las percepciones de las personas, sobre sus representaciones de la realidad, sobre los juicios que de éstas se derivan y, de modo mediato, sobre los sentimientos y emociones, la motivación y la acción.

En éste orden de ideas, podríamos por ejemplo, aludir a las definiciones del concepto así:

1.1. CONCEPTO CULTURA:

A propósito del significado de este concepto, es necesario presentar las diferentes acepciones que del mismo se han realizado desde perspectivas disciplinares específicas, academias, escuelas, y tendencias teóricas, con el objeto de precisar que la definición de cultura debe ser considerada en una dimensión polisémica, es decir, dotada de múltiples lecturas y semánticas, acorde con el contexto general en el que pretende situarse o, de acuerdo al uso, adaptación o empleo que de éste

[2] TORO ÁLVAREZ, Fernando. Distinciones y relaciones entre clima, motivación, satisfacción y cultura organizacional. En: Revista Interamericana de Psicología Ocupacional, Medellín. Vol. 17 No. 2. 1998. p. 27-40

se hace como marco referencial que pretende asemejarse a los componentes, significados, diferenciaciones y escenarios de la cultura.

De esta manera, hemos seleccionado de acuerdo con nuestro interés en la investigación realizada, una selección de concepciones y/o definiciones del concepto cultura que van desde el campo disciplinar de la antropología, disciplina que le confiere a la expresión cultura una dimensión epistemológica, hasta las apreciaciones que del mismo se han hecho en las demás disciplinas sociales y humanas como la historia, sociología, la política, la economía, la administración, la geografía, psicología y el trabajo social entre otras, haciendo particular énfasis en las definiciones empleadas en el campo de las Ciencias Administrativas.

Para aproximarnos a una lectura contextual del concepto cultura se hace necesario establecer una relación biótica del hombre y la cultura, en la cual, la evolución del hombre sugiere que no existe una naturaleza humana independiente de la cultura; sin la existencia de los hombres no hay cultura, pero igualmente, y tal vez lo más importante, sin cultura no hay hombres. O, como lo expresa C. Geertz[3] "[…] somos animales incompletos o inconclusos que nos completamos o terminamos por obra de la cultura, y no por obra de la cultura general sino por formas en alto grado particulares de ella".

1.2. LA CULTURA Y EL HOMBRE

La cultura suministra el vínculo entre lo que los hombres son intrínsecamente capaces de llegar a ser y lo que realmente llegan a ser uno por uno. Llegar a ser humano es llegar a ser un individuo y llegamos a ser individuos guiados por

[3] GEERTZ, Clifford. La interpretación de las culturas. Buenos Aires: Gedisa. 1990. 289p

esquemas culturales, por sistemas de significación históricamente creados en virtud de los cuales formamos, ordenamos, sustentamos y dirigimos nuestras vidas. Y los esquemas culturales no son generales sino específicos.

Asimismo, podemos relacionar el análisis del concepto cultura en una perspectiva mucho más amplia y en la cual, se establecen los referentes sobre los que se han desarrollado los elementos que articulan el concepto cultura con distintas dimensiones – si se quiere, adjetivaciones – en campos como la teoría organizacional, prácticas cotidianas, actitudes, formas de comportamiento, contextos específicos, etc.

En este sentido, la definición desarrollada por Clifford Geertz[4], propugna por una precisión de corte esencialmente semiótico, que junto con Max Weber precisa que el hombre es un animal inserto en las tramas de significación que él mismo ha tejido, considerando en consecuencia, que la cultura es esa urdimbre creada por el hombre en sus distintas interacciones sociales y, cuyo análisis en la práctica, debe ser por lo tanto, no desde una ciencia experimental en busca de leyes, sino en una perspectiva interpretativa en busca de significaciones. En definitiva, como precisa Geertz[5], la cultura es un documento activo; es público, y en este sentido, al verla como una acción simbólica, se debe dejar de lado la intención de hacer de ella una conducta estructurada o pensar que es una estructura de la mente, pues en esta dirección el problema de si la cultura es “objetiva” o “subjetiva” y perdería toda importancia.

[4] IBID, p. 65-72

[5] IBID, p. 148

En este orden de ideas, el profesor Luís Francisco Rivas[6], manifiesta que el análisis sobre la cultura debe trascender una lectura en la cual sea vista básicamente a partir de universos y sistemas simbólicos, lo que significa que su contextualización debe evidenciarse como un sistema de actividades humanas soportadas por sus propios componentes, o sea, que la cultura se puede leer en la lógica de su articulación como totalidad de las actividades humanas y como un conjunto de factores, en los cuales podemos analizar sus implicaciones y tener herramientas para determinar su evolución, sus entradas, salidas, procesos y sus elementos.

En consecuencia el proceso dinámico que sufre la cultura esta soportado por el conocimiento que diariamente se adquiere por parte de los miembros de una sociedad, conglomerado humano o, de una organización determinada. Este conocimiento debe ser compartido para que permita una retroalimentación y evolución de la cultura, las formas de transmitirla y compartirla como conocimiento colectivo, son una de las premisas permanentes en su evolución cotidiana a través del paso de los años.

De ahí, que para acceder a su comprensión, debemos tener presente que la cultura se dimensiona contextualmente no como complejos de esquemas concretos de conducta –costumbres, usanzas, tradiciones, conjuntos de hábitos-, como ha ocurrido en general hasta ahora, sino como una serie de mecanismos construidos a propósito de la interacción y controles socioculturales generados por la misma sociedad. Por lo tanto, la evolución del hombre sugiere que no existe una naturaleza humana independiente de la cultura; es decir, que sin la existencia de

[6] RIVAS D., Luis Francisco. Cultura organizacional. En: Memos de Investigación, Santafé de Bogotá: Universidad de los Andes. No. 107, 1993. p.2

los hombres no hay cultura, pero igualmente, y tal vez lo más importante, sin cultura no hay hombres como termina por concluir el profesor Oscar García.[7]

Así, pues, la cultura suministra el vínculo entre lo que los hombres son intrínsecamente capaces de llegar a ser y lo que realmente llegan a ser uno por uno. Llegar a ser humano es llegar a ser un individuo y llegamos a ser individuos guiados por esquemas culturales, por sistemas de significación históricamente creados en virtud de los cuales formamos, ordenamos, sustentamos y dirigimos nuestras vidas. Y los esquemas culturales no son generales sino específicos.

De otro lado, la definición hecha por Charles Taylor[8] basa la noción de cultura como un todo complejo que incluye los conocimientos, las creencias, el arte, la moral, el derecho, las costumbres y todas las demás capacidades y costumbres adquiridas por el hombre como miembro de una sociedad, dando una perspectiva que intenta delimitar los contenidos que pueden ser considerados como constitutivos de su interpretación.

Asimismo, según el investigador Carlos Eduardo Méndez[9] de la Universidad del Rosario, concluye que la literatura administrativa ha adoptado de la sociología el concepto de cultura que contempla en su definición aspectos referidos al conjunto de valores, creencias, ideologías, hábitos, costumbres y normas que comparten los individuos en la organización y que surgen de la interrelación social, los cuales

---

[7] GARCÍA VARGAS, Oscar Humberto. La cultura humana y su interpretación desde la perspectiva de la cultura organizacional. En: Pensamiento & Gestión, Barranquilla: Universidad del Norte. No. 22. 2007. p. 151

[8] TAYLOR, Charles. Una Antropología de la Identidad. Buenos Aires: Ed. Eunsa. 2002. 342p.

[9] MÉNDEZ ÁLVAREZ, Carlos Eduardo. Transformación cultural en las organizaciones: Un Modelo para la Gestión del Cambio. Bogotá: Ed. Limusa. 2009. p.78

generan patrones de comportamiento colectivos que establecen una identidad entre sus miembros y los hace diferentes de otra organización.

En otra lógica, pero aludiendo a similares apreciaciones, la enciclopedia internacional de las ciencias sociales define cultura como las "formas de comportamiento, explícitas o implícitas adquiridas y transmitidas mediante símbolos y constituye el patrimonio singularizado de los grupos humanos, incluida su plasmación en objetos; el núcleo esencial de la cultura son las ideas tradicionales y especialmente los valores vinculados a ellas".

Dos antropólogos norteamericanos, A. L. Kroeber y Clyde Kluckholn[10], interpretando y consolidando elementos contenidos en definiciones de diferentes autores concluyen que "[…] la cultura consiste en formas de comportamiento explícitas o implícitas, adquiridas y transmitidas mediante símbolos y constituye el patrimonio singularizado de los grupos humanos". Asimismo, Ward H. Goodenough[11] encuentra que la cultura "[…] no es un fenómeno material, no consiste en cosas, gentes, conductas o emociones, sino que es más bien la organización de esas cosas; la forma de las cosas en la mente del pueblo, sus modelos para percibirlas, relacionarlas e interpretarlas".

Ralph Linton[12] define la cultura como la suma de conocimientos, de actitudes y de modelos habituales de comportamientos que tienen en común y que transmiten los

---

[10] KROEBER, A.; KLUCKHOHN, C. Culture. A Critical Review of Concepts and definitions. In: Papers of the Peabody Museum, Cambridge, Harvard University Press. Vol. XLVII: 1. 1952. p.37

[11] WARD H. Goodenough. Description & Comparison in cultural Anthropology. Aldine Transaction, 2006. p.12

[12] LINTON, Ralph. Cultura y personalidad. México. Fondo de cultura Económica. 2005.p.124

miembros de una sociedad en particular. Según E.B. Taylor[13], podemos entender por cultura "[…] esta totalidad compleja que incluye el conocimiento, la creencias, el arte, la moral, la ley, la costumbre, y cualquier otro hábito y capacidad adquirido por el hombre como miembro de la sociedad". La cultura incluye "[…] todo aquel complejo que abarca el saber, la fe, el arte, la moral, el derecho, la costumbre y todas las demás capacidades y costumbres adquiridas por el hombre en su carácter de miembro de la sociedad".

Para B. Malinoswki[14], al referirse a ésta, afirma que "[…] cultura evidentemente es el conjunto integral constituido por los utensilios y bienes de los consumidores, por el cuerpo de las normas que rigen los distintos grupos sociales, por las ideas y las artesanías creencias y costumbres, ya consideremos una muy simple y primitiva cultura o una extremadamente compleja y desarrollada, estaremos en presencia de un vasto aparato, en parte material, en parte humano o en parte espiritual, con el que el hombre es capaz de superar los concretos, específicos problemas que lo enfrentan". Asimismo, la cultura es la "[…] elaboración de cosas que no aparecen originariamente en la naturaleza y, al mismo tiempo, también lo elaborado mismo; elaboración por cierto, mediante el trabajo y la utilización de conocimientos técnicos que se adquieren a través de un largo período de tiempo".

Para Kroeber y Kluckhohn[15] "[…] la cultura consiste en patrones implícitos y explícitos a través de comportamiento adquirido y trasmitido a través de símbolos, constituyendo un logo distintivo de grupos humanos, incluyendo su personificación de artefactos; el núcleo esencial de la cultura consiste en las ideas, tradiciones y

---

[13] TAYLOR, Edward B. "La ciencia de la cultura". En: KAHN, J. S. (comp.): El concepto de cultura, Barcelona: Anagrama. 1995. p. 24

[14] MALINOWSKI, Bronislaw. Los argonautas del Pacífico Occidental. Barcelona: Península. 1985. p.50

[15] KROEBER, A.;KLUCKHOHN, C., Op.Cit., p. 25-28

especialmente los valores que vienen unidos a ellas; los sistemas de cultura deben por una parte ser considerados como productos de acción y por la otra como elementos condicionales de una acción futura". Para Levi-Strauss[16], la cultura está determinada por sistemas simbólicos colectivos, por tanto es una construcción que hace la mente del hombre y de esta forma los fenómenos culturales que aparecen en la sociedad son el resultado de procesos mentales subconscientes.

Adicional a lo anterior, la lógica que asume la cultura puede igualmente observarse en términos más amplios, esto es en el plano de lo que se ha denominado como el sistema cultural, que en su conjunto y en el juego cotidiano tiene relación con el aprendizaje que el individuo hace a través de hechos observables, que percibe por si mismo en su experiencia dentro de la organización. En otras palabras, el sistema cultural influye en la creación de la conciencia colectiva de los miembros de la organización y es un reflejo, entre otros, del concepto que tiene el líder acerca del hombre en la sociedad, las organizaciones y en la estructura social en general. Por ello, es necesario igualmente tener presente que si bien existe una articulación como la descrita, también se deben precisar los elementos que permiten diferenciar el sistema social del cultural. El sistema social se diferencia del sistema cultural por que el primero concierne a las condiciones que entran en juego al establecer la acción entre individuos reales, quienes forman colectividades concretas, mientras que el sistema cultural se refiere a los valores, ideas, etc., implicados en la acción social.

[16] LEVI-STRAUSS, Claude. Antropología estructural: Mito, sociedad, humanidades. Barcelona: Editorial Paidós Ibérica. 1986. p.142

El profesor Carlos Méndez[17], afirma que el sistema cultural es un conjunto de actitudes que tienen los individuos ante ciertas situaciones o personas, y que son producto del aprendizaje en el diario vivir; permite el aprendizaje por medio de los mayores, a través de hechos observables y percibidos, que conducen a su internalización por medio de la interrelación a diario con personas y grupos a los que pertenece; ajusta la conducta de los individuos a la realidad de su grupo de referencia; regula el comportamiento en un grupo de individuos. No obstante, las definiciones de los sistemas sociales y culturales están insertas en el marco de la vida social y, por supuesto, de la sociedad en su conjunto, sin embargo en una perspectiva mucho más amplia, las anteriores definiciones y otras nociones de autores acerca del concepto de cultura se encuentran implícitas en la definición que propone Ralph Linton[18], antropólogo norteamericano, quien la visualiza como la conformación de la conducta que es aprendida y de los resultados de la misma, cuyos elementos son compartidos y transmitidos por los hombres que componen una sociedad.

En esta definición se encuentra incluido en la conducta todo aquello que aprende y produce el hombre por su actividad, refiriéndose a lo social, lo psicológico y lo físico. Tales resultados de la conducta se manifiestan en la primera instancia a través de unos rasgos inmateriales que se expresan en todo aquello que el hombre aprende por la socialización (proceso de aprendizaje social), dando lugar a los valores, actitudes, formas de pensar, sentir y obrar. En segundo lugar, por lo que puede denominarse los rasgos materiales, conformados por aquellos objetos que el hombre construye y que se manifiestan por la tecnología, la infraestructura, los inventos, etc.

---

[17] MÉNDEZ ÁLVAREZ, Carlos Eduardo. Metodología para describir la cultura organizacional: estudio de caso en una empresa colombiana del sector industrial. En: Universidad y Empresa, Santafé de Bogotá: Universidad del Rosario. No. 7. 2004. p.51-81

[18] LINTON, Ralph., Op.Cit., p.124

Algunos estudiosos de las ciencias sociales, inspirados en este concepto de Linton, proponen la cultura como el conjunto de rasgos materiales e inmateriales que caracterizan e identifican a una sociedad. Las diferentes definiciones sobre el concepto de cultura en antropología y sociología permiten identificar elementos comunes a dicho concepto que sirven para su comprensión:

- Es conciencia colectiva (se expresa por un sistema de significados compartidos), construida y compartida por los miembros de una colectividad.

- Al ser conciencia colectiva es un sistema abstracto no tangible, percibido y aprendido por la mente del hombre, quien por la socialización (aprendizaje social), construye significados mentales que le permiten comprender y adaptarse al medio en el que desarrolla sus procesos de interacción social.

- Propone el marco en el cual desarrolla la acción social, entendiendo por este las condiciones que el individuo encuentra para establecer procesos de interacción social en los que está implícita la comunicación.

- El sistema de significados por lo que se manifiesta la cultura (conciencia colectiva), influye significativamente en el sistema de personalidad del individuo determinando su comportamiento, así como sus formas de pensar, sentir y actuar en el sistema social al que pertenece y que la produce.

- No es viable, no es posible materializarla en aspectos materiales e inmateriales, estos son sus manifestaciones dando lugar a la cultura manifiesta o explícita. Fundamentalmente la cultura está en la mente de los individuos, quienes en su proceso intelectual conforman el sistema de significados, los valores, las

ideologías que de manera inconsciente y por procesos cognoscitivos se los apropian de la sociedad o los grupos a los que pertenecen.

Puede visualizarse para su comprensión en tres estadios diferentes. El primero está conformado por los rasgos materiales que el hombre produce y por las manifestaciones en el comportamiento de los rasgos inmateriales. El segundo, de carácter intermedio, en el que hay un nivel alto de conciencia formado por los valores. El tercero es invisible e influye en las formas de pensar y actuar de los individuos. Por este último el individuo hace para sí características de la cultura que refuerza con su conducta. Al respecto George M. Foster[19] en su obra Antropología aplicada afirma que la mayor parte de los hombres son ajenos a las premisas implícitas de su propia cultura, incluso cuando empieza a interiorizarlas en la vida cotidiana sin tomarlas en cuenta. Sin embargo, tal como sucede con el lenguaje, el hombre actúa como si las tuviera presentes de manera consciente y continua.

La cultura no son los valores, las ideologías, las creencias, las normas, los ritos, los mitos, los símbolos, el lenguaje, etc. estas son manifestaciones de la misma que difieren según el grupo social que los produce por su acción social.

La cultura se manifiesta a través de todo aquello que produce el hombre para satisfacer sus necesidades y vivir en sociedad (la tecnología, los inventos, la infraestructura, etc.)

Por último, y luego de haber mostrado un panorama conceptual y teórico sobre los referentes que permiten definir el concepto de cultura y sus articulaciones contextuales con lo social y con la sociedad, abordaremos a continuación uno de

[19] FOSTER, George M. Antropología Aplicada. México: Fondo de cultura Económica. 1974. p.54

los usos más recurrentes de éste concepto que para los efectos específicos del objeto de estudio de nuestra investigación se convierte en el soporte fundamental de nuestra hipótesis de trabajo, es decir la definición de la cultura organizacional.

1.3. CULTURA ORGANIZACIONAL

Para abordar esta temática es necesario precisar dos conceptos que articulados permiten acceder al sentido específico de su episteme, es decir, a los campos semánticos en los que se desenvuelven y, obviamente, en las dimensiones que adquieren y connotan. De ahí pues que debemos partir de lo que entendemos y debemos contextualizar como organización. Para Carlos Méndez[20], la organización se define como un ente social en el que tienen presencia elementos que por su existencia pueden configurarse como condiciones para la acción social, aspectos formales como la estructura, las relaciones de autoridad y poder, los procedimientos, la comunicación, las estrategias, las políticas, los estilos de liderazgo, el clima organizacional percibido y otros, determinan las relaciones sociales entre sus miembros. De esta manera, las organizaciones pueden operar bajo diferentes lógicas que en la práctica, responden a dos racionalidades, es decir, a una de orden valorativo o axiológico, que alude a valores, normas, filosofía o, sencillamente a los principios rectores de la misma; adicionalmente poseen una racionalidad instrumental u operativa cuya orientación está signada a los aspectos funcionales de la organización.

En estas condiciones, al ser definida como un ente social, las organizaciones, le confieren a sus miembros distintos roles, responsabilidades, deberes y derechos

[20] MÉNDEZ ÁLVAREZ, Carlos Eduardo., Op.Cit., p.54

que le permiten a los individuos resolver tanto sus necesidad constitutivas como parte de la organización y las necesidades mismas de ésta, o sea, del sentido funcional y valorativo que hacen que éste último haga parte del la organización. Dicho en otros términos, la diferencia que existe entre los individuos que constituyen el cuerpo instrumental y la materia pensante de éstas que por ser parte fundamental de un sistema social semejante, comparten patrones de comportamiento que en el marco de consenso social señalado anteriormente puede definirse como la conciencia colectiva de la organización o la personalidad y la identidad de la misma.

Sin embargo, ha sido desde el marco del pensamiento de las ciencias de la administración, donde las precisiones sobre lo que es, significa y contiene una organización en contexto en el cual debe situarse la reflexión sobre las mismas, pero también sobre los individuos que la componen. De tal suerte que cada que se aluda a las organizaciones debe iniciarse por hacer referencia al pensamiento Tayloriano, que contempla una diferenciación entre los integrantes de la organización, cuyo sentido está dado porque algunos de ellos son los que piensan y otros son los que hacen, lo cual expresa de manera contundente la nula participación que cierto tipo de colaboradores tenían en el aporte acerca de cómo deberían desarrollarse ciertas actividades trascendentales al interior de la empresa. En consecuencia, "[…] los integrantes de una organización proceden de un orden social espontáneo (la sociedad) y entran a formar parte de un orden social creado (la empresa), y los comportamientos de esos integrantes no necesariamente se ven afectados sólo por ese orden social creado; por el contrario, hay una alta dosis de decisión de comportamiento influenciado por el orden social espontáneo al que pertenece cada integrante que llega a la empresa".[21]

[21] GARCÍA VARGAS, Oscar Humberto., Op.Cit., p.155-156

En estos términos, las interacciones entre los miembros de la organización se reproducen en el marco del mismo significado de las relaciones sociales, es decir, se interactúa, se hacen intercambios, se llega a consensos o a disensos, se persiguen objetivos comunes y, funcionalmente se desarrollan diferentes roles al interior de la organización. Así, Oscar García[22], concluye que la organización establece relaciones sociales con sus compañeros de trabajo y otras personas, para satisfacer sus necesidades individuales y cumplir con los objetivos organizacionales (estructura social); se comporta y actúa en las condiciones propias de la estructura social de la organización (sistema social), influenciado por los valores y otros significados compartidos (sistema cultural), donde aprende y adquiere rasgos que determinan su personalidad (sistema de personalidad-conciencia individual) y que se manifiestan en su forma de pensar, sentir y obrar (acción social) y responden a las expectativas de consenso que sobre su conducta ha construido la organización (conciencia colectiva). De esta manera, Eduardo Rodríguez[23], precisa que en el juego cotidiano de los intercambios, de las lógicas y funciones que le dan sentido a la existencia de las organizaciones, terminan por convertirlas en espacios dinámicos para la praxis, o sea, para reflejar las acciones constituyen el producto de sus reflexiones, de las maneras como se articularán a los entornos que les son propios o en los que pretenden incursionar, y que en la práctica, generan las directrices para pensar cómo se actúa a través de su propio lenguaje, lenguaje que no es solamente ordenamiento de palabras en códigos o normas, sino formas de ser y/o hacer, más aún, son los hechos que devienen sentido, que construyen sentido.

---

[22] IBID., p.55

[23] RODRÍGUEZ D., Eduardo. Los laberintos del cambio organizacional. En: Revista Colombiana de Psicología, Santafé de Bogotá: Universidad Nacional de Colombia. No. 3. 1994. p.66-72

En consecuencia, las organizaciones direccionan su propia visión del mundo, toda vez que diseña sus principios, la manera como formará sus cuadros personales, la capacitación que éstos demandan y que el medio reclama, de ahí, que algunas personas piensen y "[…] difundan lo que el gran resto debe hacer, mientras tanto en esa gran masa se mueven otros actores más anónimos pero con propuestas más "afines" a la vida de ese gran "resto de gente" y con ellos crean sus símbolos y diseñan códigos paralelos de acción: en síntesis, generan sus propias culturas que se superponen a la cultura oficial de la que no se es partícipe".[24]

En este contexto se pueden proponer juegos de relaciones preestablecidas al interior de las organizaciones con otras, que dicho de paso, están determinadas por los entornos específicos donde se desenvuelven y cotidianamente se direcciona el devenir de dichas organizaciones. Así pues, los referentes que establecen las relaciones al interior de cada complejo (entendidas las organizaciones como sistemas) empresarial o institucional, sean de carácter público o privado, ofrecen al analista o al investigador diferentes panoramas que deben dimensionarse para poder establecer diferencias y marcos de comparación de lo que hemos denominado líneas atrás, como sus propias visiones del mundo y las relaciones entre ellas y los contextos donde interactúan.

De esta manera, cada organización define sus referentes culturales, sus universos simbólicos, sus políticas y estrategias de administración, pero también, cada uno de los aspectos de su ethos empresarial, es decir, de los valores, axiomas, principios y alcances, no sólo como un sistema autopoiético, sino también con relación al universo de los bienes y/o servicios que oferta en entornos específicos o que en la práctica, compiten con otros oferentes en el mercado, sea cual sea su naturaleza. Por lo tanto, esas particularidades endógenas, se constituyen en la

[24] RODRÍGUEZ D., Eduardo., Op.Cit., p.69

identidad que sus miembros comparten, leen y viven a diario, pero al mismo tiempo, son los elementos que se proyectan hacia los otros como los universos exógenos donde se reafirman y diferencian de otras organizaciones.

En este orden de ideas, las representaciones en las que se leen los miembros de una organización permiten compartir horizontes y metas colectivas, pero también dar cuenta del grado de reconocimiento y/o de pertenencia que los miembros de éstas tienen y, en la práctica poder medir o evaluar los resultados de esa imagen e identidad proyectada hacia fuera y al interior de éstas, o sea, de lo que distintos especialistas han denominado como la cultura organizacional.

Podemos, pues, entender por cultura organizacional:

> […] la conciencia colectiva que se expresa en el sistema de significados compartidos por los miembros de la organización, que los identifica y diferencia de otros, institucionalizando y estandarizando sus conductas sociales. Tales significados y comportamientos son determinados por el concepto que el líder de la organización tiene sobre el hombre, la estructura, el sistema cultural y el clima de la organización, así como por la interrelación y mutua influencia que existe entre éstos.[25]

No obstante, buena parte de los aspectos descritos dependen irrestrictamente del papel que dentro de las organizaciones juegan quienes las direccionan, bien como gerentes, administradores, asesores, consultores, etc., pero siempre, bajo la óptica de alcanzar los objetivos, planes, metas, políticas, estrategias, misión, visión, entre otros, pero bajo el espectro de alcanzar logros y por supuesto, resultados acorde a los derroteros previamente establecidos o diseñados por

[25] MÉNDEZ ÁLVAREZ, Carlos Eduardo., Op.Cit., p.54

quien dirige o quien funge como líder de la organización. Así las cosas, la cultura organizacional termina por ser el producto a veces consensuado y, otras, impuesto por el cerebro rector de las mismas y, en consecuencia, la cultura organizacional termina por convertirse en un contexto aleccionador, controlador y vigía frente al desempeño y variables que definen instrumental y axiológicamente la cultura organizacional.

Por estas razones debemos tener presente que:

> […] la cultura es un conjunto de elementos, más o menos tangibles producidos y, sobre todo, poseídos por la organización. Dicho de otra manera, la organización tiene una cultura al igual que posee una estructura o una tecnología. La cultura es una variable organizacional que moldea la identidad de la empresa […] Cuando se habla de cultura organizacional puede inferirse que el sistema de significados compartidos por los miembros de la organización es la manifestación de esa conciencia colectiva, definida por Emilio Durkheim.[26]

El discurso de la "cultura organizacional" en la práctica, para la dirección empresarial, se sitúa en toda una tradición de medios o de fórmulas ideológicas empleadas por los dirigentes para garantizar que las acciones de los miembros de la empresa tiendan a servir a sus propios objetivos. Este medio para manipular el comportamiento, y ganar la cooperación de los trabajadores, tiene la ventaja de proporcionar a quienes la utilizan una apariencia de legitimidad. La cultura se convierte claramente en un elemento en los procesos de demarcación y control que se practican en las organizaciones. Es un elemento de la ideología administrativa, ya que los administradores la utilizan conscientemente para obtener el apoyo que permita el logro de sus objetivos.

---

[26] GARCÍA VARGAS, Oscar Humberto., Op.Cit., p.159

La cultura se presenta entonces como un nuevo medio de control y de dominación, ya sea por el control de lo informal, o de la irracionalidad. Esta última noción siempre se ha asociado a lo simbólico y a lo imaginario. Según Oscar García[27], la cultura como instrumento de gestión permite la manipulación de los artefactos de tal manera que esta irracionalidad tiende hacia la racionalidad que caracteriza al proyecto gerencial. Sin embargo, no podemos confundir que tanto la cultura organizacional como el concepto más amplio de cultura que hemos precisado sean lo mismo, es decir, que respondan a los parámetros que les son propios a cada uno de ellos, esto es, universos contextuales específicos que en la práctica terminan por articularse, pero jamás por yuxtaponerse.

La cultura organizacional se desarrolla mediante un proceso de interacción de las personas que conforman una organización. El discurso y otras prácticas son los elementos que permiten el dinamismo de la cultura a través de un constante intercambio y de compartir las experiencias diarias. Su potencial está en proveer un estilo de trabajo y en permitir la flexibilidad de la estructura organizacional. Identificando los factores que conforman esta cultura se puede dirigir y fomentar el estilo de trabajo que redunde en beneficios para la organización, para sus miembros y para la sociedad. En otras palabras, son manifiestas las diferencias entre cultura y cultura organizacional, en la cual, se hacen presentes los referentes identitarios y societales de la organización y en la consciencia colectiva de sus miembros pero que en la práctica, terminan por influenciar y ser influenciados por otros componentes, tanto del orden instrumental y operativo como del orden constitutivo de los valores de tal cultura organizacional.

[27] IBID, p.164

De lo anterior podemos cotejar que ambas racionalidades no riñen entre sí, pero nos sitúan en el marco del análisis contextual que permite diferenciarlas, pero a su vez, tener presente que la cultura organizacional posee entonces diferentes niveles y componentes que además de tener las características descritas, están definidas por variables y por indicadores que nos permiten medirla, evaluarla, planificarla y adaptarla a los cambios del entorno y a las necesidades del sistema organizacional como tal.

En términos más precisos, la cultura de la organización podrá describirse teniendo en cuenta elementos tales como variables, que por la sinergia que desarrollan permiten alcanzar un nivel de comprensión suficiente para orientar acciones de fortalecimiento o transformarla. El profesor Oscar García[28], define a continuación cada variable identificada como influyente en la cultura organizacional. La definición planteada por este autor explicita cuatro variables: 1. El concepto que el líder tiene acerca del hombre, 2. La estructura, 3. El sistema cultural, 4. El clima organizacional.

1.3.1. El clima organizacional

El clima organizacional es variable de la cultura organizacional, en razón a que influye en los comportamientos del individuo y es factor determinante de la conciencia colectiva.

1.3.1.1 Definición de clima organizacional

Al analizar las definiciones sobre clima organizacional de diferentes autores se identifican elementos comunes así:

[28] IBID. p.60-66

- Describe características de la organización que la diferencia de otras.
- Es el resultado de las conductas y comportamientos percibidos por el individuo.
- Incluye los aspectos formales e informales propios de la organización. Informales que orientan los comportamientos de los individuos y, a su vez, crean percepciones subjetivas sobre el ambiente de trabajo.
- Produce actitudes y conductas que señalan el grado de motivación del individuo.

Puede entenderse por clima organizacional:

> […] el ambiente propio de la organización, producido y percibido por el individuo, de acuerdo a las condiciones que encuentra en su proceso de interacción social y en la estructura organizacional, el cual se expresa por variables (objetivos, motivación, liderazgo, control, toma de decisiones, relaciones interpersonales, cooperación) que orientan su creencia, percepción, grado de participación y actitud, determinando su comportamiento, satisfacción y nivel de eficiencia en el trabajo.[29]

1.3.1.2. Relación entre cada una de las variables influyentes para describir la cultura organizacional:

Las cuatro variables inciden en la construcción de la cultura organizacional. Su relación e influencia producen la conciencia colectiva, que el hombre proyecta en sus comportamientos y que, de una u otra forma, incide en los niveles de eficiencia y productividad.

---

[29] CONTRERAS, Francoise. Leadership: Prospects for Development and Research. In: International Journal of Psychological Research. 2008. p. 42. ISSN 2011 – 7922.

Un ejemplo ilustra la relación entre las variables propuestas como influyentes, en la creación de la cultura organizacional. Para ello se tomó como referencia la primera variable influyente:

El concepto que el líder tiene sobre el hombre:

- El sistema cultural de la organización es, en buena medida, determinado por el líder. Algunos de los mitos, ritos, creencias, historias, se construyen sobre el tipo de relación que el líder establece con sus empleados; aspectos como el grado de reconocimiento y motivación que proporcione a sus empleados son explicables en este contexto.
- Influye sobre la estructura por que sobre su visión se establecen las relaciones de poder y el ejercicio de la autoridad, los niveles jerárquicos, la forma como se da o no la descentralización, delegación y coordinación; la comunicación y otros componentes sobre los que la estructura adquiere una dinámica que es propia de cada organización, y sobre los que se construye una conciencia colectiva que orienta el comportamiento de los individuos.
- El líder es un factor determinante del clima organizacional. La visión que tiene del hombre influye no solamente en la construcción del sistema cultural y en la estructura de la organización, sino que, además, produce percepciones en el individuo que, traducidas en clima organizacional, influyen en su desempeño y motivación en la empresa

La empresa desarrolla acciones orientadas al desarrollo de sus empleados, mediante programas de capacitación y estrategias que les permitan participar en los procesos, propiciando y reafirmando acciones fuera de la rutina y repetición de labores en el desempeño de su cargo, creándoles satisfacción y sentido de compromiso con el trabajo realizado. Para ampliar los componentes y las variables

de la cultura organizacional pueden verse los siguientes trabajos Jorge Etkin[30], Richard Nholan[31], Luis Francisco Rivas[32], María Teresa Echavarría[33] y Antonio Pérez García.[34]

Estos modelos mentales colectivos conforman la globalidad de los principios que gobiernan una organización y que deben ser conocidos por todos los miembros. Estos modelos permiten entender las acciones tomadas por las personas y proveen el marco para actuar en una forma coherente. Se puede pensar en los modelos mentales como la base mínima de conocimiento y cultura compartida en una organización.

En síntesis, las diferentes variables que constituyen el soporte de la cultura organizacional están definiendo no sólo la estela de valores y acciones de la misma, sino también están modelando esquemas discursivos, mentales y de comportamiento que en la práctica, operan como un todo estructurado, o sea, como la organización en sí misma. El comportamiento lo podemos ver como un conjunto de reglas de inferencia, que nos permitan deducir verdades a partir de los axiomas que nos facilita el paradigma que culturalmente adopte la organización, para desempeñarse ante la sociedad.

---

[30] ETKIN, Jorge. La Doble Moral de las organizaciones. Sistemas Perversos y Corrupción Institucionalizada. México: Mc. Graw Hill Editores. 1994. ISBN-10: 8448101456

[31] NHOLAN, Richard. Destrucción Creativa. México: Mc. Graw Hill Editores. 1996.

[32] RIVAS D., Luis Francisco., Opt.Cit., 20p.

[33] ECHAVARRÍA J., María Teresa. Componentes de la cultura organizacional. En: Pensamiento & Gestión, Barranquilla: Universidad del Norte. No. 9. 2000. p.42-55.

[34] PÉREZ GARCÍA, Antonio. De identidades y de organizaciones. En: Prisma, Montevideo: Universidad Católica de Uruguay. No. 10. 1998. p.7-41

Así, la cultura organizacional se ve como el conjunto de fenómenos que determina como una organización se desenvuelve con relación al medio ambiente y a las situaciones internas. Este conjunto de presunciones y creencias básicas deben ser compartidas por los miembros de una organización y son el producto del aprendizaje de su interacción con el entorno y de las situaciones conflictivas internas. Pero este compartir de la cultura no se da por falta de un diálogo dirigido y ésta cultura no evoluciona por falta de una retroalimentación basada en el conocimiento. Según Luís Fernando Rivas[35], es aquí donde radica el problema del mayor número de empresas que no tienen éxito.

El contexto general de la cultura organizacional, dependerá entonces como producto del equipamiento mental, funcional y axiológico de la organización toda vez que logre consolidar y mantener un clima organizacional que mas allá, de ser una necesidad de la misma, debe ser el producto y evidencia del buen direccionamiento y administración de los componentes y recursos con los que cuenta la organización. Por lo tanto, otro de los aspectos teóricos y conceptuales que abordamos en nuestra investigación, se fundamenta en la impronta dimensional de toda organización establecida por la importancia y búsqueda permanente de un clima organizacional óptimo, adecuado y vital, como producto mismo de esa cultura organizacional que hemos descrito.

De ahí pues, que una organización pueda verse a sí misma como un equipo o familia que cree en el trabajo en común. Y todavía otra puede estar altamente fragmentada, dividida en grupos que ven el mundo de muchas y variadas formas o que tienen diferentes aspiraciones de lo que una organización podría ser. Tales patrones de creencias compartidas, divididos o integrados, y soportados por varias

[35] RIVAS D., Luis Francisco., Op.Cit., p.6

normas operativas y rituales, pueden ejercer una influencia decisiva en la eficiencia de la organización para conseguir los retos que afronta.

Uno de los modelos más fáciles de apreciar la naturaleza del clima organizacional es simplemente observar el funcionamiento cotidiano de un grupo de organizaciones al que pertenezcamos como si fuéramos foráneos a ellas. Las características del contexto organizacional observado gradualmente se harán evidentes y, además, la manera como se hacen conscientes los modelos de interacción entre los individuos, los lenguajes que emplean, las imágenes y temas de conversación y los variados rituales de la rutina diaria. Al explorar las razones de estos aspectos normalmente se encuentran explicaciones de tipo histórico en cuando al modo de hacer las cosas y en general al clima organizacional.

La noción de clima organizacional se estructura en un gran número de obras que sugieren conceptos y definiciones semejantes a la noción de cultura preconizada por la escuela cognoscitiva. El clima allí se concibe como una percepción tenaz y general de los atributos esenciales y del carácter del sistema organizaciones. En síntesis, para el profesor Luís Francisco Rivas[36], es el mapa cognitivo del individuo, elaborado con experiencias personales dentro de la organización y que suministra al miembro señales esenciales para poder adaptar se comportamiento a las exigencias y los objetivos de la organización.

El clima es, pues, una forma de competencia aprendida que permite al individuo interpretar las exigencias de la organización y comprender sus propias interacciones cotidianas con la organización y sus miembros.

[36] IBID. p.6-8

Las organizaciones se convierten así en artefactos sociales que resultan de mapas cognitivos compartidos por los miembros. Ellas son la expresión de un espíritu colectivo, el cual es más que la suma de los espíritus individuales que la componen. “Esta noción de espíritu o mente colectiva es bastante ambigua; se trataría de una representación distinta pero enlazada (pero de una manera oscura e imprecisa) a las representaciones individuales de los miembros de la organización”[37]

Se acaban de plantear de forma detallada los principales elementos que permiten definir la cultura como concepto, las diferentes propuestas teóricas alrededor de ésta, asimismo, desde las teorías organizacionales la apreciación sobre el concepto de organización y de cultura organizacional. Estos parámetros nos dan una idea precisa de los temas, los soportes y los contenidos que en términos generales, nos permitirán desarrollar nuestra hipótesis de trabajo sobre la seguridad de tecnología como una variable de la cultura organizacional.

1.4. Seguridad de Tecnología Informática (TI)

Ahora, en relación al tema específico de seguridad de TI la mayor cantidad de bibliografía existente es de carácter técnico. En este orden de ideas, la seguridad de TI, es el tema en las áreas de informática de “moda”, toda vez que en los últimos años, las empresas se han volcado a trabajar fuertemente sobre este particular, debido a que gran parte están intercomunicadas entre ellas o a Internet, lo que hace que potencialmente estén expuestas a pérdidas o alteraciones de información.

---

[37] ÁBRALE; ALLAIRE y OTROS. Cultura organizacional. Aspectos teóricos prácticos y metodológicos. Bogotá. LEGIS, 1992. p.16-18.

La seguridad de TI tiene cantidad de información e investigaciones pero orientadas principalmente en el aspecto tecnológico y en este sentido, hay permanentes investigaciones y desarrollos para tratar de lograr niveles de seguridad óptimos en la información de las empresas. A nivel mundial, todos los días hackers, crackers o personal especializado en seguridad descubren vulnerabilidades o desarrollan nuevos modelos y métodos de ataques para lograr accesar la información de las empresas, pero esas investigaciones se han centrado en lo tecnológico y han desarrollado variedad de equipos o plataformas cuya función principal es contraatacar las violaciones y los ataques que le realizan a las redes.

Como ya se mencionó anteriormente, casi la totalidad de información sobre seguridad de TI, es de tipo técnico, por ejemplo, hay información sobre cómo implementar tácticas para la detección de virus, procedimientos para asegurar los sistemas operativos de los computadores personales (PCs) y los servidores, sistemas para controlar ataques, sistemas de seguridad perimetral (en los sistemas que conectan a las redes corporativas con otras empresas o Internet), etc. En definitiva, se puede afirmar que existen gran cantidad de manuales sobre seguridad de TI.

En Colombia hay empresas que se dedican a la seguridad de TI, algunas de ellas son: Unisys, KPMG, eTeck, Cyberia, entre otras que ofrecen servicios técnicos especializados para lograr óptimos niveles de seguridad en las empresas, pero en la práctica, éstas orientan su trabajo en esquemas de aseguramiento informacional.

El ISO (The International Organization for Standardization) y el IEC (The International Electrothecnical Commission) publicó un estándar internacional que

es la norma ISO/IEC 17799 (Information Technology – Code of Practice for Information Security Management), ésta se ha convertido en la norma a seguir en todas las compañías alrededor del mundo, su objetivo principal es lograr un código formal para la gestión de la seguridad de la información.

Las empresas en Colombia que trabajan en seguridad prácticamente tienen como objetivo implementar la norma ISO 17799 en las empresas que ellos asesoran, al implementar la norma se logra obtener procesos, procedimientos y tecnologías que aseguran la plataforma. Adicionalmente, hay sitios en Internet especializados en facilitar herramientas teóricas, de software, etcétera cuyo objetivo es ayudar a las empresas a implementar la norma ISO 17799.

En Colombia las legislaciones sobre tecnología han ido evolucionando lentamente, existen leyes y decretos publicados por el gobierno, algunos son: Ley 527 DE 1999[38], por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones; Decreto número 1747 de 2000[39], por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales; Circular Externa 052 de 2007[40] de la Superintendencia Financiera de Colombia que imparte instrucciones relacionadas con los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y

---

[38] OBSERVATORIO COLOMBIANO DE CIENCIA Y TECNOLOGÍA (OCYT). Ley 527 de 1999. <http://www.ocyt.org.co/leg/Ley%20527.pdf> [citado en junio 09 de 2009]

[39] MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO. Decreto número 1747 de 2000. <http://www.mincomercio.gov.co/eContent/documentos/normatividad/decretos/decreto_1747_2000.pdf> [citado en junio 09 de 2009]]

[40] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular externa 052 de 2007. <http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf> [citado en junio 09 de 2009]

canales de distribución de productos y servicios para clientes y usuarios; Ley 1273 de 2009[41], por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado "De la protección de la información y los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones; Decreto número 1524 de 2002[42], que regula el acceso a Internet a sitios con contenidos que atenten contra la moral y adecuado desarrollo de los menores de edad. Existen otras leyes y disposiciones legales sobre el tema de la seguridad, la penalización en el código penal colombiano como la Ley 599 de 2000[43], la revisión de derechos de autor en la Ley 603 de 2000[44] y Ley estatutaria 1266 de 2008[45], por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

---

[41] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html> [citado en junio 09 de 2009]

[42] MINISTERIO DE COMUNICACIONES – REPUBLICA DE COLOMBIA . Decreto número 1524 de 2002. <http://www.cntv.org.co/cntv_bop/basedoc/decreto/2002/decreto_1524_2002.html> [citado en junio 09 de 2009]

[43] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 599 de 2000. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html> [citado en junio 09 de 2009]

[44] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 603 de 2000. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0603_2000.html> [citado en junio 09 de 2009]

[45] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley estatutaria 1266 de 2008. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html> [citado en junio 09 de 2009]

Se ha especulado mucho que para alcanzar una verdadera seguridad de TI no sólo es necesario la implementación de cantidad de aspectos técnicos como: procedimientos, políticas y equipos que se logra mediante la adecuada implementación de la norma ISO; también es necesario una cultura de seguridad al interior de las organizaciones, sobre ésta, dentro del desarrollo de la investigación y del rastreo bibliográfico realizado no se encontraron trabajos precisos o que por lo menos aludieran al tema de manera referencial, en consecuencia, hacemos mención de unos pocos sitios en los cuales se pueden encontrar alusiones relacionadas al desarrollo de una cultura de seguridad de TI, pero no se específica en qué consiste la cultura de seguridad de TI o cómo lograr consolidar ésta al interior de las organizaciones. Las organizaciones han invertido décadas tratando de equilibrar redes más abiertas, más extensas y mejor conectadas con defensas más fuertes contra intrusos, incluyendo firewalls, software antivirus, biometría y controles de identidad para el acceso. "Estas medidas han hecho que el mundo de los negocios sea más eficaz en detener las amenazas desde el exterior, y han hecho que cada vez sea más difícil para los futuros piratas informáticos o los virus irrumpir en los sistemas. Estas tecnologías, sin embargo, son mayoritariamente pasivas en su modus operandi y han sido diseñadas para frustrar únicamente el acceso no autorizado; proporcionando sólo una primera línea de defensa".[46]

Es allí donde ubicamos el planteamiento del problema de la investigación y los objetivos propuestos en el proyecto para demostrar nuestra hipótesis de trabajo, es decir, la seguridad de tecnología de información (TI) como una variable de la cultura organizacional, toda vez que las evidencias empíricas nos permiten afirmar

---

[46] IBM CORPORATION. Detener los ataques internos: cómo pueden proteger las organizaciones su información confidencial. <http://www-05.ibm.com/services/es/cio/pdf/CIO_Series_0302.pdf> [citado en septiembre 1 de 2006]

que, uno de los problemas más frecuentes en buena parte de nuestras empresas, tanto del sector secundario como del terciario, han padecido y enfrentado problemas relacionados con el adecuado manejo de sus sistemas de información y con las tecnologías empleadas en este sentido; en otras palabras, la mayor parte de los ataques que se realizan para robar o alterar información se ejecutan al interior de las organizaciones y con una adecuada cultura de seguridad de TI incorporada al ethos organizacional se lograría prevenir este flagelo, que como lo atestiguan informes especializados de empresas y consultores en seguridad, ha venido incrementándose significativamente en los últimos años.

> […] reveló que el 33% de los ataques contra la seguridad de la información fueron perpetrados por empleados internos, mientras que el 28% procedían de antiguos empleados y socios; Cada año se realizan más transacciones comerciales electrónicamente y las organizaciones guardan un volumen cada vez mayor de información confidencial. Para muchas organizaciones, la información se ha convertido en un activo de incalculable valor, en la parte vital de sus operaciones. El acceso a esta información está al alcance de una base de usuarios en expansión, incluidos los empleados, socios comerciales, proveedores y clientes. Las infraestructuras de TI son cada vez más amplias, más complejas, más fraccionadas, y más accesibles. Esta interconexión ofrece muchas ventajas para empresas, organismos gubernamentales y consumidores similares pero, al mismo tiempo, introduce posiblemente una gran dosis de riesgo. Cuantos más puntos de acceso tenga una organización, mayor es la vulnerabilidad de los sistemas y la posibilidad de sufrir robo de datos. Y los riesgos son altos, especialmente como depositarios de información privada. Las empresas y organismos gubernamentales deben cumplir con estrictos requisitos normativos y proteger el capital intelectual ante competidores y entidades políticas subversivas. Y los consumidores son por lo general los que están

> más preocupados ante una posible usurpación de identidad y otras violaciones de privacidad. La creciente preocupación pública por la seguridad y la privacidad de los datos personales ha situado a muchas empresas y organismos gubernamentales en el centro de atención; y muchos países de todo el mundo han elaborado normativas concebidas para preservar la confidencialidad. Las leyes del Reino Unido, como la Ley de Protección de Datos de 1998, han evolucionado en los últimos años con el fin de combatir el fraude y la usurpación de identidad. En Estados Unidos, el estado de California aprobó su Ley de Notificación de Infracción contra la seguridad que exige a las empresas (sea cual fuere su ubicación geográfica) que revelen los casos de violación de datos relacionados con ciudadanos del estado de California. Desde entonces, otros 23 estados han aprobado sus propias leyes de revelación de información. Y Canadá tiene la intención de adoptar medidas similares. Estas acciones legislativas recientes, así como las frecuentes noticias en los medios sobre infracciones contra la seguridad, han hecho que tales amenazas adquieran una clara preponderancia.[47]

Entre otras, una de las razones fundamentales que justifican la articulación de la seguridad de TI como constitutiva de la cultura organizacional se basa en es la aplicación del control en el área de informática se debe a la creciente dependencia de las industrias y empresas de producción, de servicios y de educación, en los equipos de computación, en el software, en el procesamiento de la información, en la vulnerabilidad creciente de los sistemas, en el costo de las actuales y futuras inversiones en recursos informáticos, en los dramáticos cambios organizacionales que puedan acarrear las nuevas tecnologías, todo ello debido a que el uso de las computadoras conlleva riesgos de errores, omisiones, fraudes y otros sucesos

[47] BERINATO, Scott. The Global State of Information Security 2005. Pricewaterhouse Coopers and CIO <http://www.cio.com/archive/091505/global.html> [citado en septiembre 15 de 2005]

adversos, que ameritan su permanente control y supervisión en mayor grado a los procesos que se llevan manualmente, para garantizar la confiabilidad, confidencialidad y seguridad de los sistemas de información; es por ello, que para lograr el éxito y supervivencia de las organizaciones, es necesario contar con una efectiva administración de la tecnología informática, que pueda responder adecuadamente a los problemas anteriormente señalados.

En estos términos, la seguridad de TI de las organizaciones, van de la mano con los diferentes aspectos del cotidiano devenir, es decir, cómo sobrevivir, cómo relacionarse, cómo interactuar en distintos contextos y entornos, en la práctica termina por ser instintos básicos, y las organizaciones no escapan de estos principios. En este orden de ideas, en la práctica, las organizaciones están acostumbradas a manejar la seguridad física como parte fundamental de la operación del negocio. Cerraduras, celadores, perros, etc., son prácticas muy comunes en nuestros días para la protección de la infraestructura física. No existe un nivel completamente seguro que garantice proteger todos los riesgos a los cuales se puede ver avocado un negocio. Los problemas de seguridad casi siempre están asociados al error humano, por ignorancia, por falta de compromiso, pertenencia, responsabilidad, cultura u omisión con la organización de la cual se hace parte. Por otro lado, el enemigo regularmente está dentro de la organización.

En la mayoría de los casos de fraudes informáticos, éstos se realizan con apoyo interno. En muchos casos, las organizaciones desarrollan costosos mecanismos para aislarse y protegerse de ataques externos y se olvidan de la amenaza interna. Alcanzar un equilibrio entre los controles y la funcionalidad es clave para mantener la competitividad del negocio. La seguridad informática no debe ser vista sólo como un problema técnico, para cualquier organización de hoy en día, la información es un activo de los más preciados**,** y la operación se basa

principalmente en sus facilidades computacionales y en servicios informáticos hacia sus clientes.

2. MARCO TEÓRICO

2.1. SEGURIDAD DE TECNOLOGÍA: CRITERIOS GENERALES, CONCEPTOS Y PREMISAS:

En múltiples investigaciones realizadas se considera el tema de la seguridad de TI como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad tal como lo afirma el Ph.D. Jeimy Cano[48]. Al revisar la inseguridad informática como estrategia de pensamiento estratégico reconocemos que un sistema es tan seguro como su falta de seguridad más reciente, que cuando ocurre o se manifiesta un problema de seguridad las personas se vuelven más experimentadas y saben que hacer, que los sistemas mal diseñados (pensamiento natural en seguridad informática) no están preparados para fallar (pensamiento dual en inseguridad informática). En pocas palabras, mantener a tus amigos cerca pero más cerca de tus enemigos.

El concepto de la organización como una mente pensante y actuante, con un pensamiento complementario (dual) nos sugiere que la seguridad de TI, como una distinción más de la organización, representa una dinámica de acción que podríamos recrear considerando los elementos de la mente segura sugeridos por Day[49], una mente segura consiste en la revisión y práctica de virtudes y reglas de

[48] CANO, Jeimy J. Inseguridad informática: Un concepto dual en seguridad informática. En: Revista de Ingeniería, Bogotá: Universidad de los Andes. No. 19. 2004. p. 40-44

[49] DAY, K. Inside the security mind. Making the tough decisions. Prentice Hall. 2003. p.5.

seguridad con el fin de tomar decisiones claras, consistentes y efectivas. Complementario a esta propuesta, el Dr. Cano[50], expresa que la existencia de una menta insegura, como realidad presente de la organización, es un punto de análisis adicional que se considera, no solo para dar sentido a la práctica de las virtudes y reglas de seguridad, sino para mantener la perspectiva de la incertidumbre inherente al proceso de la seguridad informática.

Las virtudes de la seguridad son: la seguridad debe ser una consideración diaria, la seguridad debe ser un esfuerzo comunitario, las prácticas de seguridad deben mantener un foco generalizado, las prácticas de seguridad deben incluir medidas de entrenamiento para todo el personal de la organización y ser constitutivas de los principios rectores del clima, misión y visión organizacional, esto es, componente vital de la cultura organizacional. Las reglas de seguridad son: regla del menor privilegio. Regla de los cambios, regla de la confianza, regla del eslabón más débil, regla de separación, regla de los tres procesos, regla de la acción y regla de la respuesta apropiada e inmediata. Los sistemas informáticos de las empresas actualmente necesitan estar interconectadas entre ellas o con Internet, como ya se había mencionado. Al haber una gran expansión de Internet y que cada día haya más y más usuarios conectados a la red mundial ha hecho que el riesgo de conectar las empresas sea mayor.

En razón a lo anterior, la mente insegura, al igual que la inseguridad informática son parte de un mismo continuo que busca entender que la seguridad de TI como necesidad organizacional, no es mas que el resultado de una propiedad emergente de un sistema que conoce sus condiciones extremas, su operación límite, así como sus recursos y posibilidades para darle sentido a la razón de su misión.

---

[50] CANO, Jeimy J., Op.Cit., p.42-43

Considerar la inseguridad informática como parte del ejercicio de seguridad de TI de las organizaciones, sugiere la capacidad de las organizaciones para cuestionarse sobre la situación real del balance entre seguridad, facilidad de uso y funcionalidad para lograr mayores niveles de confiabilidad y aseguramiento de sus arquitecturas, sino para evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar los medios de protección. Las organizaciones no buscarán solamente incrementar la confianza de sus clientes, sino comprender que la seguridad no es un problema de tecnología, sino un problema de riesgos y las diferentes maneras de comprenderlos y manejarlos. Así, mientras más se conoce la inseguridad informática más se comprenden las acciones y resultados de la seguridad en las organizaciones concluye el profesor Cano[51].

En un contexto internacional articulado por la compleja y cambiante realidad de un mundo interconectado se abre necesariamente la puerta a la reflexión divergente que con frecuencia se escucha en las organizaciones. De un lado, la gerencia en su lenguaje se pregunta "¿por qué los de seguridad informática tienen que hacerlo todo más fácil?, y, por otro, la voz de los ingenieros de seguridad de la información manifiesta que "con esos requerimientos cada vez más complejos de la gerencia, sin considerar los impactos en la infraestructura, tendremos que sacrificar seguridad por funcionalidad". Dos posiciones, dos mundos, dos lenguajes, dos formas de entender el mismo problema; la información y el negocio. De esta manera, mas allá de las políticas de planeación, de la relación costo/beneficio, y del marco general de la cultura organizacional, se hace evidente una dicotomía entre dos universos colindantes –la dirección y sus equipos de trabajo- que debe ser resuelta y que sea capaz de sopesar las dualidades del lenguaje mencionadas y mas bien, sea el producto relacional del deber ser de las organizaciones que en

[51] IBID, p.43

nuestra perspectiva se fundamenta en la consolidación de la seguridad de TI como una de las variables constitutivas de la cultura organizacional.

En otros términos, esta dicotomía es una reflexión de dos contrarios que se complementan y se vuelven uno. Por un lado, la información nace, se transforma, se almacena, se recupera y se dispone desde los procesos de negocio; y, por otro, el negocio no se puede manejar sin la información y sin la generación de datos que den cuenta de lo que ocurre en el aspecto productivo. En tal sentido, asegurar o proteger el negocio, debe llevarnos a proteger la información y viceversa.

Así las cosas, la cultura organizacional en torno de la seguridad de TI se basa en la práctica en las mismas lógicas de lo que significa administrar los negocios corporativos, que en la realidad cotidiana termina por ser necesariamente la administración de la información. No obstante, alrededor de esta dicotomía y/o complementariedad funcional, buena parte del acervo científico publicado sobre el tema de la seguridad y los negocios, se establecen una serie de mitos (que llamaremos "[…] Leyendas Empresariales Digitales (LED)"[52], frente a las que prácticamente, académicos y gerentes se sienten perturbados y confrontados ante una realidad de eventos que estas pueden o no confirmar. A continuación, detallaremos cinco de las principales LED que se escuchan frecuentemente en la comunidad de la seguridad de la información:

- **LED No. 1. "Los directivos no saben de seguridad de la información"**
  La sabiduría convencional advierte que esto es cierto, pero la no convencional nos dice que el problema no es que este nivel de la organización no conozca de seguridad, sino que, por una parte no es consciente de los riesgos, y por otra, que los profesionales de la seguridad no han sabido vender la distinción.

[52] IBID, p.56-58

- **LED No. 2. "El usuario no es consciente de la protección de su información"**

  La sabiduría convencional nos dice que los usuarios son descuidados e inmaduros y muchas veces ingenuos.
- **LED No. 3. "No es viable desarrollar métricas de seguridad, dado que es un mundo muy cambiante"**

  La sabiduría convencional nos dice que las métricas son esas "excusas numéricas" que utilizan los administradores, para mostrar la evolución de su gestión en términos generalmente cuantitativos. Decir que no es viable desarrollar métricas por lo dinámico del entorno, es reconocer el poco entendimiento del bien que se administra y del modelo de calidad que toda organización debe tener. Desarrollar métricas, particularmente en seguridad de la información, es meditar en aquellas preguntas que se deben responder; es pensar en el futuro con los pies en el presente y ver cómo se recorre el camino desde la inseguridad a la confiabilidad de los sistemas.

- **LED No. 4. "La gerencia no habla el lenguaje de la seguridad, solo el de los negocios"**

  La sabiduría convencional nos muestra que el gerente es gerente y nada tiene que ver con la seguridad. Pero la sabiduría no convencional, nos sugiere hacer un ejercicio de *"rompimiento de un sistema de cifrado";* un ejercicio para identificar los patrones de la seguridad de la información en las decisiones de negocio; dejar de utilizar el paradigma técnico y táctico, para utilizar el de los procesos y las relaciones, como motivación básica para observar el sistema de seguridad emergente que plantea la dinámica de la organización
- **LED No. 5. "A mayor inversión en tecnologías de seguridad, mayor confianza"**

  Esta leyenda empresarial se debe más a la sensación, sentimiento y percepción. Muchos gerentes de seguridad se "sienten" en paz-tensa cuando

saben cuáles nuevas tecnologías se están empleando para mejorar el estado de la seguridad, un logro de su gestión que les permite menos márgenes de incertidumbre. Pero la sabiduría no convencional indica que la confianza se gana enfrentando y superando las situaciones críticas; mostrando la capacidad de acción y la preparación de un equipo para afrontar y controlar una falla inesperada. Confiar en las tecnologías de seguridad, presupone la preparación de la función de seguridad en una postura de falla segura.

Adicional a esto:

[…] las organizaciones deben evaluar paradigmas de protección tales como:

- Qué es lo que se pretende abordar: seguridad en la infraestructura de TI o seguridad de la información, en la cual se contemplan elementos como (seguridad física, seguridad de los empleados, seguridad de los procesos).
- Visión de la seguridad desde el punto de vista técnico, o servicio de apoyo a los servicios de negocio de la organización.
- Enfoque y orientación a procesos y procedimientos.
- Arquitecturas de servicios orientadas a la seguridad y protección de los activos de información de la organización.
- Entrenamiento y conciencia organizacional sobre la seguridad de la organización o si sólo las áreas de tecnología deben poseer dicha conciencia y, Gobierno corporativo en torno a la seguridad de la organización.
- Gobierno corporativo en torno a la seguridad de la organización.[53]

[53] ALMANZA J., Andrés Ricardo. Responsable de la inseguridad de la información. En: SISTEMAS, Santa Fe de Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 105. Abril-Junio 2008. p.63-64

En consecuencia, más allá de lograr hacer precisiones en lo que significa la relación dual o no descrita, entre la dirección de una organización y su capital humano, de lo que se trata es de inferir los referentes puntuales sobre los cuales debemos consolidar una cultura organizacional que esté soportada de manera integral y dinámica en las lógicas derivadas de la seguridad de TI, con lo cual su lectura como variable del ethos empresarial nos permitirá no solo sopesar su importancia sino corregir en el tiempo y con prontitud cualquier clase de problemas internos o exógenos al devenir de nuestras empresas u organizaciones en ésta materia.

De lo anterior podemos pues inferir la necesidad de conjugar ese soporte de una cultura de la seguridad de TI sobre una visión sistemática de la misma, esto es, aquella que busca identificar la inseguridad de la información en el marco específico de la evolución de las vulnerabilidades en los diferentes mecanismos tecnológicos, asimismo, hacer consciencia y poder leer la falta de compromiso de las organizaciones con el tema de seguridad y la existencia de una limitada cultura del cuidado de la información como común denominador de buena parte de éstas (que en buena medida es otro argumento justificatorio de la imperiosa necesidad de fundar como constitutiva de la cultura organizacional, la seguridad de TI), se establece el escenario ideal para que la inseguridad desarrolle todo su potencial, un escenario donde la función de la seguridad no tiene la variedad requerida para identificar la inseguridad, ni comprenderla.

En este contexto, comprender el "trinomio clásico de la seguridad de la información: confidencialidad, integridad y disponibilidad"[54], se hace una labor desafiante y desconcertante, pues cada una de las fallas de seguridad

[54] CANO, Jeimy J. Administrando la confidencialidad de la información. En: SISTEMAS, Santa Fe de Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 101. Julio-Septiembre 2007. p. 62-69

identificadas podría corresponder a múltiples escenarios y variables que superan la capacidad de atención y operación de la función de seguridad, en definitiva, si no ha sido incorporada la seguridad como un elemento identitario del deber ser de las organizaciones, seguiremos pensando en sistemas y soluciones técnicas que seguirán siendo meramente operativas e instrumentales, pero para nada sustrato garante de la cultura organizacional.

No obstante, para lograr desarrollar consecuentemente una cultura organizacional que comprenda, lo que significa, pero sobre todo, que se base en la seguridad de TI sería aquella capaz de resolver lo más preocupante que podemos encontrar en la mayoría de las organizaciones, y es que muchas veces los sistemas de información de una compañía no son vulnerados desde el exterior, protegidos en su punto de acceso a Internet mediante firewall y programas antivirus, sino que son los mismos empleados de las empresas quienes constituyen la mayor amenaza de riesgo informático. ¿Cómo? Sencillamente, porque en la mayoría de los casos ellos tienen acceso a la red interna de una manera desmonitorizada, es decir, sin valorar el significado que como conocimiento tiene la información y, en consecuencia, sin hacer seguimientos sistemáticos basados en indicadores de uso y empleo que de ésta hacen los miembros de la organización.

> […]Hoy en día, el activo más valioso de una organización son sus intangibles, la mayoría de los cuales se pueden encontrar en sus bases de datos.[55]

Estas bases de datos, que han tomado tiempo, esfuerzo y recursos en desarrollarse con frecuencia están libremente expuestas en la red interna al

---

[55] CALDAS LEMAITRE, Rodrigo. Seguridad informática ¿Una política empresarial? En: SISTEMAS, Santa Fe de Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 89. Julio-Septiembre 2004. p.1-2

alcance de los usuarios, sin ningún tipo de restricciones, con la posibilidad que estos las “hurten” sin que nadie se dé cuenta. Y en esto debemos ser cuidadosos. El delito de hurto generalmente se configura cuando el legítimo dueño pierde la posesión del bien y el ladrón la adquiere. El problema es que en el robo de información, la posesión de la misma por parte del dueño original no se pierde. El dueño de la base de datos la sigue teniendo en su disco duro, y tal vez nunca note que le han robado la información. Lo más grave es que la información en si misma no es propiedad, y como tal no puede ser objeto de hurto –lo que se roban es el arreglo de la base de datos, no la información que contiene la misma- mediante la simple copia.

Así mismo, el profesor Rodrigo Caldas[56], aclara que con un simple dispositivo de memoria USB se pueden grabar información desde un gigabyte, hasta un terabyte en disco portable externo, más que suficiente para llevarse toda la base de datos de cualquier empresa. Y nadie se dará cuenta del asunto si la organización no tiene las herramientas de monitoreo y seguimiento adecuadas o el hecho se percibe cuando es demasiado tarde, sin embargo, más allá del simple ejercicio de prevención, cuidado, vigilancia, monitoreo y control del uso y del manejo de las bases de datos y de la información, se trata es de sopesar las conductas irregulares en materia de seguridad de TI, hasta llegar a consolidar un modelo de trabajo inherente al devenir cotidiano de las organizaciones, hasta afianzarlo como parte vital, axiológica e instrumental de la cultura organizacional, es decir, de construir un modelo de seguridad basado en los principios mismos del ethos misional de la empresa y, que en términos de políticas y estrategias de planeación y proyección de las organizaciones, respondan al ejercicio identitario de dicha cultura, de la imagen y del clima organizacional.

[56] IBID, p.2

En otras palabras, si de la seguridad de TI se partiera para consolidar una cultura de la organización, habría que hacer de las prácticas de la primera un universo de referentes simbólicos en los cuales se identificaran y pudieran leer todos los miembros de la organización y como resultado de ello, expresiones, comportamientos empresariales, lenguajes, formas de hacer y de pensar la misión organizacional estarían atravesadas de manera integral por todos y cada uno de los elementos que constituyen el modelo que soporta dicha estructura de seguridad de TI.

Lo anterior ha generado que las empresas tomen iniciativas orientadas a asegurar sus redes informáticas y sobre todo la información y conocimiento que existen al interior de las empresas. Estas iniciativas están orientadas a implementar la norma ISO/IEC 17799 o su versión actualizada en la norma ISO/IEC 27000-series, a contratar empresas que les hagan auditorias de seguridad y que les diseñen procesos, políticas e implementen equipos de seguridad todo lo anterior con el fin de lograr unos niveles de seguridad altos para evitar que se hagan robos o alteraciones en la información. El Anexo 3, es un resumen de la norma ISO/IEC 27000-series en donde se especifica cuales normas la componen y que áreas cubre cada una de ellas.

2.2. LA CULTURA DE SEGURIDAD DE TECNOLOGIA DE INFORMACIÓN (TI)

Un primer elemento y por demás, uno de los más importantes, es la cultura de seguridad de TI. Una cultura está compuesta por tres componentes: los artefactos, lo que se observa (lo que se ve, lo que se siente y escucha), símbolos y comportamientos; los valores expuestos, es decir, lo que le dicen y finalmente, los supuestos básicos, aquello que los participantes dan por hecho. Según la premisa

anterior, el doctor Jeimy Cano[57], concluye que cultura es la base fundamental de la gestión de la seguridad, entendida ésta como la promoción inherente y natural de comportamientos confiables de las personas que permitan interiorizar la distinción de prácticas de protección coherentes con las políticas internas, el fortalecimiento de una percepción y administración del riesgo, el convencimiento de autocuidado, los impactos financieros de acciones inseguras y sobre manera, el interés y entendimiento propio de las regulaciones que sobre el tema se tienen.

Además, el doctor Cano[58], afirma que la cultura de seguridad de la información debe ser el animador y custodio de variables tan importantes para las organizaciones como su reputación, los ingresos, el cumplimiento regulatorio, la percepción del cliente y los flujos de información en los procesos.

> "[..] Si bien las buenas prácticas son parte inherente de la evolución de la gestión de la seguridad de la información, cada organización, en su dinámica de negocio, debe comprender los riesgos a los cuales se encuentra expuesto y responder de acuerdo con este diagnóstico [..] la necesidad de contar con un sistema de control interno informático que permita la evolución permanente y constante de los sistemas de gestión de seguridad de la información, basados en una administración inteligente de los riesgos, una comprensión de la dinámica de la inseguridad y la validación de los controles actuales que la organización establece para operar de manera confiable".[59]

---

[57] CANO, Jeimy J. Monitoreo y evolución de la seguridad de la información. En: SISTEMAS, Bogotá: Asociación Colombiana de Ingenieros de Sistemas-ACIS-. No. 110. Abril-Junio 2009. p.4-13

[58] IBID, p.8

[59] SCHNEIER, B. Security and compliance. En: IEEE Security & Privacy, USA. July/August. 2004. p.3.

Como referencia bibliográfica para ampliar la lectura sobre las prácticas de seguridad como soporte de la cultura organizacional, se puede consultar el documento “Securing the whole enterprise: Business and legal issues” escrito por TANEY Jr., F. y COSTELLO, T.[60]

En este orden de ideas, es necesario aludir a la importancia que al respecto debe tener la seguridad de las aplicaciones, es decir, el desarrollo de estudios que apunten de manera sistemática a reducir todo tipo de acciones menos inseguras, o sea, tener presente que ésta es una práctica emergente derivada de las prácticas generales de ingeniería de software. Aunque, no han sido establecidos estándares sobre la seguridad del software y debido a la contundencia de las fallas de los programas en las empresas, ha repercutido positivamente a que tanto las organizaciones como las industrias tomen conciencia de los mismos y procuren hoy mejores soluciones informáticas para las organizaciones.

> […]Es claro que el software sin errores o fallas está muy lejos de la realidad, pero lo que sí es claro, es que se hace necesario establecer métricas que permiten ubicar un punto en el tiempo para saber dónde estamos y qué tenemos, y los niveles de aseguramiento de información que deseamos para las soluciones tecnológicas futuras.[61]

Sumado a lo anterior, al abordar el tema de la seguridad de TI, debemos considerar, que en un mundo globalizado, donde las dinámicas de las tecnologías e innovaciones informacionales, transforman los sistemas de intercambio y la circulación de intangibles (información) bajo la variable de la velocidad en la Red,

---

[60] TANEY Jr., F.; COSTELLO, T. Securing the whole enterprise: Business and legal issues. En: IEEE IT Professional, USA. January/February. 2006. p. 8-9.

[61] CANO, Jeimy J. Monitoreo y evolución de la seguridad de la información., Op.Cit., p.9

se hace vital para abordar contextualmente los problemas que se derivan de ello, tener presente la existencia de lo que los expertos han dado en denominar como los incidentes de seguridad que, en la práctica, se visualizan como la única constante en el mundo de las organizaciones y en consecuencia, la seguridad ha orientado toda su atención a los incidentes como norma general de la gestión de seguridad de la información.

En otras palabras, las organizaciones consideran que un incidente se puede definir como una cadena sucesiva de aplicaciones inadecuadas en las prácticas mismas de seguridad, que podemos observar como aquellos eventos que materializan en una serie de consecuencias colectivas y, lo que es peor, terminan por materializarse en los miembros y equipo de la empresa como una creencia que responde a un apetito natural por el riesgo de las personas y sus acciones.

Al respecto, este tipo de actitudes y de prácticas de gestión y/o de trabajo en las organizaciones terminan por ser consideradas por Jorge Etkin[62] como prácticas desviadas del deber ser de una cultura organizacional, toda vez que se hacen bajo un marco de Opacidad, esto es, asumidas como riesgo individual pero atentatorias contra la misión, visión y productividad de toda la organización. Así las cosas, los incidentes se asumen sin las precauciones adecuadas y en consecuencia, los resultados de los mismos pueden ser fatales para las empresas.

De lo anterior podemos inferir que, todos los aprendizajes que de estas realidades se obtengan, deben beneficiar y fortalecer una cultura de seguridad de la información basada en el reporte abierto y oportuno de las actividades inseguras, la sinceridad y transparencia de las notificaciones de los hechos eventuales y sobre manera, la firme convicción de la organización para prepararse mejor para

[62] ETKIN, Jorge. La Doble Moral de las organizaciones. Sistemas Perversos y Corrupción Institucionalizada. México: Mc. Graw Hill Editores. 1994. ISBN-10: 8448101456

disminuir los impactos de una falla parcial o total en sus operaciones de negocio. El reporte de los incidentes es la materia prima para afinar el olfato de la organización frente a la inseguridad, la formalización de la aplicación de las buenas prácticas de seguridad y la responsabilidad de cada persona frente a la información y el compromiso del área de seguridad para facilitar su buen uso en el contexto de los procesos de negocio.

No obstante, la construcción de una cultura de la seguridad como parte fundamental del deber ser de la cultura organizacional debe considerar que el proceso de afianzamiento de la misma, tiene que pasar por instaurar una serie de referentes y principios sobre los cuales se soportan los mínimos involucrados en el deber ser de una cultura de la seguridad de TI y se expresan en los siguientes aspectos.

2.2.1. Convergencia de la seguridad:

La convergencia de la seguridad, según lo define el documento, *Security Convergence and ERM*, realizado por *Alliance for Enterprise Security Risk Management*, es "la integración de manera formal, colaborativa y estratégica, de los recursos de seguridad de una organización, con el fin de entregar beneficios empresariales frente a la mitigación de riesgos, mejoramiento de la efectividad operacional, eficiencia y disminución de costos."[63]

---

[63] THE ALLIANCE FOR ENTERPRISE SECURITY RISK MANAGEMENT (AESRMT). Security convergence and ERM. The Convergence of IT Security and Enterprise Risk Management: A Security Professional's Point of View. <http://www.aesrm.org/files/Convergence_SecProf_View_5Mar09_Research.pdf> [citado en mayo 30 de 2009]. p.5

2.2.2. Consecuencias de la seguridad en la organización:

"Sin un entendimiento y mirada crítica a los patrones de tendencias en seguridad de la información, sin una adecuada interiorización de una cultura de seguridad y sin un referente particular que guíe la práctica de la gestión de la seguridad, las organizaciones estarán avocadas a ser blanco permanente de la inseguridad, de los incidentes y las implicaciones legales."[64]

2.2.3. Compromiso organización en la seguridad:

"Detallar la evolución y la monitorización de la seguridad de la información, debe ser un hábito corporativo, una responsabilidad de cada persona que participa en ella y el compromiso del área de seguridad. Una estrategia práctica y real para afianzar la gestión y el aseguramiento de la información que permita entender las motivaciones de la gerencia y así, generar valor para sus clientes."[65]

Sin embargo, a la hora de evaluar tanto la gestión como las responsabilidades en materia de seguridad, no es sorprendente que:

> […] la alta dirección traslade la mayoría de las veces la responsabilidad de la seguridad digital a su personal técnico o a los asesores de los que se contrata para "hacer que la organización sea impermeable". Así pues, este método de distanciamiento es extraordinariamente inadecuado, teniendo en cuenta todo lo que está en juego. Según estimaciones del sector, las quiebras de seguridad afectan al 90% de las empresas todos los años y generan unos costos de aproximadamente 17.000 millones de dólares.[66]

---

[64] CANO, Jeimy J. Monitoreo y evolución de la seguridad de la información., Op.Cit., p.11

[65] IBID, p.12

[66] AUSTIN, Robert D.; DARBY, Christopher A.R. El mito de la Seguridad Informática. En: Harvard Deusto Business Review. Barcelona. No. 120. Enero 2004. p. 66-74

La responsabilidad de los directivos de TI de las empresas, no solo deben ser los gerentes técnicos, ellos son principalmente los responsables de una violación de seguridad de TI, por ese motivo no deben dejar el trabajo únicamente el personal técnico sino que además deben asumir un papel más proactivo y ser los verdaderos líderes del proceso de seguridad de TI, principalmente con el manejo de las medidas preventivas y proactivas en el menor tiempo posible, y esto es debido a que cada vez mayor la cantidad de ataques internos en las organizaciones.

> […]Las buenas noticias son que no hace falta que los directores generales estudien los aspectos más misteriosos de los sistemas de TI de sus empresas para establecer las principales medidas preventivas. A diferencia de los directores de TI, que si pueden verse obligados a participar más directamente en el juego del gato y el ratón con los potenciales intrusos, los altos directivos empresariales deberían fijarse en la tarea de gestionar el riesgo, tarea con la que ya están familiarizados. Su función debería ser evaluar el valor que tienen para la empresa sus activos de información, determinar las probabilidades de que puedan estar comprometidas y adaptar a la medida un conjunto de procesos que atenúen el riesgo para hacer frente a puntos débiles específicos. Este método, que concibe la seguridad informática como un desafío operativo, más que como un desafío técnico, podría asimilarse a los programas clásicos de garantía de la calidad, en el sentido de que trata de evitar, más que de arreglar, los problemas y en el sentido de que requiere la participación de todos los empleados, no sólo del departamento de tecnologías de la información. Lo que se pretende no es que los sistemas informáticos sean absolutamente seguros, tarea imposible, por cierto, sino reducir el riesgo empresarial a un nivel aceptable y empoderar en la práctica, una variable de la cultura

organizacional, como de hecho lo es, la seguridad de tecnología de información (TI).[67]

En síntesis, la seguridad se ha convertido en un tema de crucial importancia para el continuo y espectacular progreso de nuestro mundo e incluso para su propia supervivencia, tal y como ahora lo vivimos. Prueba de ello es que las más importantes empresas multinacionales tienen catalogada a la seguridad de la información como alta prioridad estratégica.

2.2.4. Plan de seguridad de la información:

Por lo que respecta a las medidas de tipo administrativo/organizativo, estas tienen que ver con la gestión de la seguridad. Deben ser previas a las medidas de tipo físico y técnico y, una vez adoptadas estas, subyacentes a las mismas. Se articulan en un plan de seguridad de la información cuyas etapas son: primero, elaboración de una política de seguridad, segundo, creación de una estructura de gestión de la seguridad, y tercero, establecimiento de los procedimientos de seguridad resultantes del desarrollo de esa política.

2.2.5. Elaboración de una política de seguridad:

La política de seguridad es al conjunto de principios y reglas que regulan la forma propia de cada organización, de proteger las informaciones que maneja.

2.2.6. Creación de una estructura de gestión de la seguridad:

A la segunda etapa, estructura de gestión, debe crearse un departamento específico encargado de gestionar la seguridad.

---

[67] IBID. p. 66-74.

2.2.7. Establecimiento de los procedimientos de seguridad:

Las funciones de seguridad estarán basadas en la colaboración y trabajo articulado con los niveles políticos de la institución en la elaboración de la política de seguridad, elaboración y mantenimiento de los procedimientos de seguridad, análisis y evaluación de riesgos, evaluación y selección de productos, concienciación y formación de usuarios, ensayos de vulnerabilidad, identificación de futuras amenazas, etc.

2.2.8. Distribución de los procedimientos de seguridad:

Los aspectos de estos procedimientos que convenga sean conocidos por todo el personal, se distribuirán en forma de manual de seguridad (muy conciso para que todos los empleados lo puedan asimilar) con ejemplares numerados en todas las páginas y con instrucciones estrictas sobre las consecuencias disciplinarias de su divulgación.

2.2.9. Éxito del plan de seguridad:

Para finalizar, merece la pena enfatizar que el éxito de cualquier plan de seguridad de la información, pasa por la directa implicación en el mismo de los máximos responsables de la institución. Son ellos los únicos que pueden impulsar las anteriores medidas de protección, que por involucrar a todos los departamentos de la entidad (no solo, y esto es muy importante, a los departamentos informáticos), requieren una decidida voluntad de los niveles de decisión más elevados de las instituciones.

En conclusión, es necesario tener presente que la cultura de la seguridad de TI, demanda una serie de cambios y de actitudes en relación a los parámetros que deben consolidarla y, también los referentes metodológicos, conceptuales, teóricos, culturales y técnicos que la soportaran. De esta forma, desarrollar cultura toma tiempo, energía y mucho compromiso. Para lograr incrementar esta cultura

se debe diseñar un fuerte programa de divulgación a través de cursos, seminarios, talleres, y otros apoyos escritos como, circulares en papel, en correo electrónico, mercadeando las medidas en mensajes cortos y efectivos. El nivel de cultura interiorizado debe ser medido regularmente a través de encuestas monitoreo de disminución de problemas de seguridad, realizando observaciones directas, etc. No obstante, la concreción práctica de la variable organizacional de la seguridad de TI, debe estar apoyada de manera integral en unos mecanismos de control cuya lógica pueda garantizar, en la práctica, la sostenibilidad, profundización y permanencia en el tiempo de dicha cultura de la seguridad. Para ello, es menester precisar los referentes sobre los cuales puede la organización controlar y garantizar la cultura de la seguridad de de TI como variable fundamental de la cultura organizacional.

2.3. ¿CÓMO DEBEMOS DEFINIR EL CONTROL?

> “Por control podemos entender el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales.
>
> El control actúa sobre las personas, cosas, situaciones específicas, fuentes de información y organizaciones, las cuales requieren con urgencia el

diseño de estrategias que le permitan controlar y corregir los resultados de sus actividades.” [68]

Si realizamos una subdivisión del control, tendríamos dos tipos de control interno y externo:

- **“Control interno**: Es aquel proceso que se ejerce internamente en las organizaciones y es impulsado por las directivas, administradores y demás personal que está vinculado a ella, el cual posee la suficiente ética y moral, así como formación académica, que le amerite credibilidad a sus hallazgos y conclusiones y tiene como propósito lograr el cumplimiento de los objetivos institucionales.

- **Control externo**: Es aquel ejercido por personal ajeno a la organización y su propósito es establecer en qué medida, los resultados alcanzados por las entidades o personas sujetas al control, satisfacen las metas y objetivos trazados en las políticas, planes, programas y propósitos fijados por la administración.”[69]

2.3.1. ¿Qué papel juega el control en los sistemas de información?

Para garantizar que los datos sean reales, exactos, oportunos, suficientes y que al ser procesados no se afecten por diferentes motivos como pérdida, omisión o redundancia, y que la información sea de utilidad en los procesos y consultas de las empresas se implementa el control en los sistemas de TI, que pueden ser:

---

[68] TAMAYO A., Alonso; DUQUE M., Néstor D. ¿Cómo se deben controlar los sistemas de información?. En: NOOS, Manizales: Universidad Nacional de Colombia. No. 18. 2004. p. 129-130.
[69] IBID, p.131.

- **“Controles generales:** Son aquellos controles ejercicios sobre las actividades y recursos comprendidos en el desarrollo de los sistemas de información e implica procesos de planeación, definición clara y precisa de metas y objetivos institucionales, definición de valores de la organización, políticas, procedimientos, estándares, gerencia participativa, apertura a la comunicación, desarrollo de equipos de mejoramiento continuo, programas de capacitación y entrenamiento, etc.

- **Controles operativos:** Son controles diseñados, desarrollados e implementados para sistemas específicos, buscando garantizar con ellos que todas las operaciones sean autorizadas, registradas y procesadas de una manera completa, exacta y oportuna y tiene que ver con control y organización de proyectos, control de flujos de información, revisiones del diseño del sistema, administración de bases de datos, controles de cambios a programas, bitácoras de cambios, mantenimiento y documentación, control de programas, reportes varios, diseño y control de formatos, comunicaciones, etc.

- **Controles técnicos:** Tiene que ver con la tecnología de la información como son los controles de operación del hardware, seguridad sobre los sistemas de información, integración de los sistemas de información, reporte de fallas, control de usuarios, restricción de accesos a datos, archivos y programas, utilización de hardware, controles lógicos del sistema, sistemas operativos, sistemas de seguridad, respaldo y confidencialidad, control de acceso al sistema, sistema de mantenimiento, planes de contingencia, etc.”[70]

En definitiva, la consolidación, evaluación y control permanente -bajo los parámetros descritos- nos permiten proponer un esquema para validar nuestra

[70] IBID, p. 130-133

hipótesis de trabajo y, que en la práctica está soportada empíricamente en la aplicación de una encuesta a diferentes tipos de empresas y organizaciones que valoran y conciben la información como un activo y recurso estratégico y económico de suma importancia. De esta manera, las variables consideradas en la encuesta se fundamentan en los referentes conceptuales que hemos definido líneas atrás al precisar cómo la variable de la seguridad de TI hace parte de la cultura organizacional. Así pues, se encuestaron empresas de diferentes sectores productivos y organizaciones de servicios financieros, inversiones y banca, construcción e ingeniería, educación, seguros, tecnología y telecomunicaciones, manufacturas e industrias de alimentos. Lo que nos permitió validar y constatar la hipótesis de nuestra investigación y lograr sugerir y proponer un modelo de seguridad que detallaremos a continuación.

2.4. FUNDAMENTOS DE UN MODELO DE SEGURIDAD INFORMÁTICA

Para el desarrollo de este modelo hicimos un análisis de los antecedentes, historia, técnicas, modelos implementados, estrategias y políticas adoptadas por distintas empresas entre otros y, una lectura crítica de los consensos que a nivel internacional han consolidado un lenguaje preciso en materia de seguridad de TI, con lo cual pretendemos proyectar nuestra propuesta de un modelo de seguridad articulado como variable a la cultura organizacional. En este orden de ideas, los aspectos que a continuación detallamos constituyen el soporte investigativo, administrativo y técnico acordado a nivel internacional para enfrentar los problemas de seguridad de TI, en el contexto específico de ésta como referente de la cultura organizacional.

2.4.1. Lecciones del libro naranja[71]

La historia de los conceptos de la seguridad en cómputo datan de 1968. El *National Bureau of Standarts (NBS)* (ahora *National Institute of Standarts and Technology-NIST*) hizo un estudio de los requerimientos de seguridad del gobierno de Estados Unidos. Ante lo alarmante del resultado del estudio de 1972, el NBS patrocinó una conferencia de la *ACM (Asociation for Computing Machinery)* sobre seguridad informática. Esta asociación es la mayor asociación profesional de especialistas en cómputo del mundo con más de 100.000 socios. La mayoría de éstos provenientes del medio académico, razón por la cual, la convocatoria del gobierno de Estados Unidos evidencia la importancia conferida a éstos como referentes precisos para evaluar y sugerir diferentes propuestas en ese sentido.

De este tipo de convocatorias se fueron diseñando estrategias en materia de seguridad y de capacitación, tanto para académicos como para empresas de distintos objetos sociales. Fue así como en 1977, el NBS inició una serie de talleres acerca de la auditoria y evaluación de sistemas de cómputo. En 1980 se responsabilizó al director de la *National Security Agency* (Agencia Nacional de seguridad) de localizar sistemas confiables de cómputo, lo que condujo en 1981 a la creación del *Computer Security Center (CSC)* del Departamento de Defensa. Finalmente, en 1983 se publicó el documento *"Trusted Computer System Evaluation Criteria"* llamado el "libro naranja". En este documento se compilaron los acumulados y la experiencia de tres décadas en el uso de las computadoras centrales compartidas por muchos usuarios y los estudios académicos y prácticos que había realizado hasta ese momento el gobierno americano. En este orden de ideas, para explicar las conclusiones de dicho libro retomamos los cuadros y las

[71] DALTABUIT, Enrique; HERNÁNDEZ, Leobardo; MALLEN, Guillermo; VÁSQUEZ, José. La seguridad de la información. México: Ed. Limusa. 2007. p.233-263.

jerarquizaciones de conceptos propuestas por (Daltabuit, Hernández, Mallen y Vásquez; 2007:234)

Tabla 1. Niveles -Libro Naranja-

B	Básico
I	Intermedio
A	Avanzado
MA	Muy avanzado
E	Extraordinario
EE	Especialmente Extraordinario

Y, la clasificación en niveles:

Tabla 2. Clasificación en Niveles -Libro Naranja-

Clase	Característica	Subclase	Característica	Descripción
A	Protección verificada	A1	Diseño verificado	Documentación y vigilancia de origen afín
B	Protección obligatoria	B3	Dominios seguros	Vigilancia ineludible y probada, soporte para la administración de seguridad, auditoria segura.
		B2	Protección estructurada	Modelos formales, canales encubiertos, control de la configuración, auditoria.
		B1	Protección con etiquetas	Modelos de políticas, etiquetas para sujetos y objetos.
C	Protección voluntaria	C2	Acceso controlado	Encapsulamiento de recursos, responsabilización lógica.
		C1	Acceso discrecional	Responsabilización lógica.
D	Protección mínima			No pasa las pruebas

El primer grupo de conceptos se refieren a las políticas y a la clasificación de la información mediante etiquetas adoptando el modelo de control de acceso de Bell-La Padula.

Tabla 3. Conceptos de políticas y clasificación de la información

	C1	C2	B1	B2	B3	A1
Control de acceso voluntario	B	I	I	I	A	A
Rehúso de objetos		B	I	I	I	I
Etiquetas			B	I	I	I
Integridad de las etiquetas			B	B	B	B
Exportación de información etiquetada			B	B	B	B
Etiquetas en la información legible			B	B	B	B
Control de acceso obligatorio			B	I	I	I
Etiquetas de clasificación del contenido				B	B	B
Dispositivos etiquetados				B	B	B

El siguiente concepto es el de responsabilización:

Tabla 4. Concepto de responsabilización

	C1	C2	B1	B2	B3	A1
Identificación y autenticación	B	I	A	A	A	A
Auditoria		B	I	A	Ma	Ma
Trayectoria confiable				B	I	I

Luego aparece el concepto de documentación como elemento de seguridad:

Tabla 5. Concepto de documentación como elemento de seguridad

	C1	C2	B1	B2	B3	A1
Manual de las funciones de seguridad para el usuario	B	B	B	B	B	B
Manual del sitio confiable	B	I	A	Ma	E	E
Documentación de las pruebas	B	B	B	I	I	A
Documentación del diseño	B	B	I	A	Ma	Ma

Llegándose así a los conceptos de garantías requeridas:

Tabla 6. Conceptos de garantías requeridas

	C1	C2	B1	B2	B3	A1
Arquitectura del sistema	B	I	A	Ma	E	E
Integridad del sistema	B	B	B	B	B	B
Pruebas de seguridad	B	I	A	Ma	e	EE
Especificación y verificación del diseño	B	I	A	Ma	E	Ee
Análisis de canales encubiertos				B	I	I
Administración confiable del sitio				B	B	I
Administración de la configuración				B	B	I
Recuperación confiable					B	B
Distribución confiable						B

2.4.2. Information Technology Segurity Evaluation Criteria (ITSEC)[72]

Asimismo, apuntando en la misma dirección en materia de seguridad el centro de *Information Technology Segurity Evaluation Criteria (ITSEC)*[73], desarrolló el que se dio en llamar como el Libro Blanco o *White Book*, en el cual se compilaron un conjunto de criterios armonizados para la evaluación de la seguridad de sistemas y productos propuestos por algunos países de Europa. De esta manera, el objetivo principal de esta publicación era proveer al usuario final de un cierto grado de confianza para que el sistema reuniera los requerimientos de seguridad necesarios y adecuados. Si comparamos los aportes de uno y otros textos (El Libro Naranja con El Libro Blanco) encontraremos tanto los lineamientos como lo que precisa cada uno de ellos en la lógica de la seguridad de TI, así:

Al igual que el TCSEC, el libro blanco define la seguridad como un conjunto de tres elementos:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

En el ITSEC todo producto o sistema es referido como: *TOE (Target Of Evaluation)*. Ambos son compuestos por elementos de Software o Hardware y la diferencia principal entre ellos radica en el entorno.

---

[72] IBID, p.233-263.

[73] OFFICE FOR OFFICIAL PUBLICATIONS OF THE EUROPEAN COMMUNITIES. Information Technology Security Evaluation Criteria (ITSEC): Provisional Harmonised Criteria. <http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf>. 1991. ISBN 92-826-3004-8 [citado en Septiembre 1 de 2009]

- Para un producto, el entorno es algo muy general, de hecho, se hacen muchas suposiciones acerca del mismo.
- Esto hace que un producto sea susceptible de ser utilizado en una gran variedad de entornos.
- Para un sistema, el entorno es muy específico, real y en teoría único.
- Así, los sistemas pueden estar constituidos por productos (quizá ya evaluados)
- Los componentes de un TOE (producto o sistema a ser evaluado) pueden estar involucrados con la seguridad o no.
- Al conjunto de componentes del TOE que tienen que ver con la seguridad se les denomina *TCB (Trusted Computing Base).*
- Un TOE debe tener definido su objetivo de seguridad *(segurity target)*:
    - Política de seguridad
    - Funcionalidades que implementan la seguridad
    - Mecanismos de seguridad
    - La fuerza de mecanismo mínima
    - El nivel de evaluación que se pretende alcanzar
- Existen diez funcionalidades definidas en el ITSEC. Estas van de la clase F1 a la clase F10.
- De la clase F1 a la F5 corresponden a las clases TCSEC.
- De las clases F6 a la clase F10 se incluyen aspectos de integridad y disponibilidad, tanto para entornos centralizados como para redes.

Para certificar un producto o sistema el proveedor:

- Presenta el documento denominado ST *(Security Target for the evaluation)*.
- En el ST se definen las funciones de seguridad del TOE, amenazas posibles y mecanismos utilizados.

- Se determina el nivel de certeza (*assurance*) que se desea alcanzar, éste se basa en buena implementación (*correctness*) de las funcionalidades de seguridad con que cuenta el TOE y que éstas sean efectivas (*effectiveness*).
- Se determina el nivel de evaluación que se desea alcanzar entre algunos de los siguientes:
  - De EO a E6, donde indica que la seguridad ofrecida por el TOE no es adecuada, y E6 denota que el TOE posee un alto grado de confianza (en cuanto a la seguridad ofrecida).
- En el proceso de evaluación, primero se determina si el TOE es correcto (*correctness*), de ser así se procede a probar su efectividad (*effectiveness*).
- La efectividad tiene que ver con que el TOE funcione adecuadamente, y que sea resistente a ataques directos.

A manera de ejemplo, el producto *"Check Point VPN-1/FireWall-1"* se anuncio en su tiempo de la manera siguiente: *"is the first IPSEC VPN to achieve ITSEC E3 Level Certification, and internationally recognized mark of product excellence"*[74]. Esto denota la importancia que ha cobrado actualmente, que los sistemas – particularmente los que proveen la seguridad en las organizaciones - demuestren la confianza que puede uno depositar en ellos y, en sus modelos.

La correspondencia aproximada entre el *"Orange Book"* y el *"White Book"* se ilustra en la siguiente tabla:

[74] CHECK POINT SOFTWARE TECHNOLOGIES LTD. Check Point VPN-1/FireWall-1 Achieves Internationally Recognized ITSEC Security Certification. <http://www.checkpoint.com/0301/itsec/>. [citado en septiembre 26 de 2009]

Tabla 7. Correspondencia entre el *"Orange Book" y "White Book"*

ITSEC	TCSEC
E0	D
F1,E2	C1
F2,E2	C2
F3,E3	B1
F4,E4	B2
F5,E5	B3
F5,E6	A1

A manera de notas finales, debe considerarse que el ITSEC incluye además de la confidencialidad, la integridad y la disponibilidad como metas de seguridad, prestando atención a los ambientes de red y no sólo a los sistemas o productos aislados, sino también, tomando en cuenta la velocidad con la que se desarrolla la tecnología en nuestros días, la evaluación con el ITSEC es más rápida y por tanto menos costosa.

2.4.3. Lista de preocupaciones

De las experiencias y resultados de las evaluaciones en materia de seguridad, tanto las agencias internacionales como el Gobierno de los Estados Unidos, han establecido los referentes que deben tenerse presente a la hora de consolidar un modelo de seguridad o de estrategias de control para instalar y constituir como fundamental dentro de los referentes de la cultura organizacional de las empresas. Así por ejemplo, las preguntas que se deben considerar para ello las podemos resumir en la siguiente lista:

¿Cómo hacemos para colocar la tecnología de información bajo control de modo que brinde la información que necesita la organización? ¿Cómo manejamos los riesgos y aseguramos la infraestructura de la que somos tan dependientes? Como son muchos los problemas que enfrenta la administración, estas amplias preguntas estratégicas generan las siguientes preguntas tradicionales a las que responderemos: ¿Cuál es el aspecto/problema? ¿Cuál es la solución? ¿De qué está constituido? ¿Funcionará? ¿Cómo lo hago?

Fue así como, una de las formas que encontraron para resolver estos problemas fue creada por el *Information Technologies Governance Institute (ITGI)* y la *Information Systems Audit and Control Association (ISACA)* en una publicación titulada COBIT: "Objetivos de Control para la información y las tecnologías Relacionadas *(Control Objetives for Information and related Technology)"*[75] dentro del Marco Referencial de COBIT. La siguiente información se transcribe según los aspectos detallados en su contenido así:

COBIT es un estándar abierto para el control de la tecnología de información, desarrollada y promovida por el *IT Governance Institute* (Instituto de Gobierno de tecnologías de información). Este marco de referencia identifica 34 procesos de tecnologías de información (TI), un enfoque de alto nivel para controlar esos 34 procesos, así como 318 objetivos de controles detallados y directrices de auditoría para evaluar los 34 procesos de TI. Provee un estándar aplicable de manera general y aceptable para buenas prácticas de seguridad y control de TI, que soportan las necesidades de la administración para determinar y monitorear el nivel apropiado de seguridad y control de TI para sus organizaciones.

---

[75] INFORMATIOM SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). Control Objetives for informatiom and related technology, 2006. <http://www.isaca.org/cobit>. [citado en Septiembre 10 de 2009].

Adicionalmente, el *IT Governance Institute* ha construido esta obra con investigación de vanguardia, en cooperación con expertos, analistas y académicos de la industria a nivel mundial. Lo anterior ha traído como resultado la definición de las Directrices Gerenciales para COBIT, que están constituidos por Modelos de Madurez, Factores Críticos del Éxito (CSFS, siglas de los términos en inglés), Indicadores Claves de Objetivo (KGIS, siglas de los términos en inglés) e Indicadores Claves de Desempeño (KPIS, siglas de los términos en inglés). Este entrega un marco significativamente mejorado que responde a la necesidad de control y mensurabilidad de TI de la administración suministrándole a la administración herramientas para determinar y medir el entorno de TI de su organización contra los 34 procesos de TI que COBIT identifica (ver la sección "Modelos de Madurez" en este documento).

Hay numerosos cambios en TI y en la construcción de redes que hacen énfasis en la necesidad de manejar mejor los riesgos relacionados con TI. La dependencia de la información electrónica y de los sistemas de TI es esencial para respaldar procesos críticos de negocio. Los negocios exitosos necesitan manejar mejor la compleja tecnología que predomina en todas sus organizaciones para responder rápida y de forma segura a las necesidades del negocio. Además, el entorno regulatorio está exigiendo un control más estricto sobre la información. Esto a su vez es direccionado por el incremento de la revelación de desastres de los sistemas de información y el incremento de fraude electrónico. El manejo de los riesgos relacionados con TI está siendo entendido ahora como una parte clave de la dirección de la empresa.

Dentro de las directivas de la empresa, el responsable y los responsables de TI se están volviendo cada vez más prominentes para el logro de los objetivos de la organización agregando valor mientras balancea el riesgo frente rendimiento sobre la TI y sus procesos. El gobierno de TI es integral para el éxito del gobierno de la

empresa asegurando mejoramientos eficientes y efectivos mesurables en los procesos relacionados de la empresa.

COBIT incluye los siguientes 39 pasos para mejorar la seguridad:[76]

1) Sobre la base del impacto sobre los procesos críticos de la empresa hay que identificar:
   a) Los datos que no deben perderse ni usarse dolosamente
   b) Los servicios que deben estar disponibles
   c) Las transacciones en las que se debe confiar (que sean auténticas e íntegras)
   d) ¿Quién puede acceder y modificar información?
   e) ¿Qué respaldos se requieren y por cuánto tiempo?
   f) ¿Qué disponibilidad se requiere?
   g) ¿Qué autorización y verificación se requieren para transacciones electrónicas?
2) Definir responsabilidades específicas para la administración de la seguridad y asegurarse de que se asignen, se comuniquen y se entiendan bien. Estimar el peligro que representa concentrar demasiados perfiles y responsabilidades en una sola persona. Asignar los recursos necesarios para que las responsabilidades se puedan ejercer efectivamente.
3) Comunicar consistentemente y discutir regularmente las reglas básicas de la implementación de los requisitos de la seguridad y de la respuesta a incidentes. Redactar listas de acciones que se deben tomar y de aquellas que no se deben tomar. Recordarles a todos los riesgos de seguridad y sus responsabilidades personales.
4) Al contratar se deben verificar las referencias.

---

[76] DALTABUIT, Enrique; HERNÁNDEZ, Leobardo; MALLEN, Guillermo; VÁSQUEZ, José., Op.Cit., p. 233-247.

5) Hacerse, reclutando expertos o vía capacitación, de los conocimientos y habilidades que se requieren para apoyar los requerimientos de seguridad de la empresa. Verificar anualmente que los conocimientos y destrezas estén actualizados y si no lo están actualizarlos.
6) Asegurarse de que ninguna tarea esencial de seguridad dependa críticamente de un solo recursos.
7) Identificar qué se tiene que hacer con respecto a las obligaciones sobre privacidad, propiedad intelectual, contractuales, normativas y de seguros. Fomentar que el personal entienda estas obligaciones y las cumpla.
8) En momentos apropiados hay que discutir con el personal clave qué puede fallar en la seguridad de la tecnología de la información que pudiera impactar en forma significativa los objetivos de la empresa. Decidir cuál es la mejor forma que los servicios, datos y transacciones críticas para el éxito de la empresa se mantengan seguros. Preparar un plan de acción de administración de riesgos para mitigar los riesgos más severos.
9) Logar que el personal entienda la necesidad de responder a los requerimientos de seguridad y determine la forma más efectiva desde el punto de vista del costo para administrar los riesgos de seguridad que se han identificado a través de buenas prácticas (buenos respaldos, control de acceso, protección contra virus, cortafuegos) y contratar seguros.
10) Prestar atención a los riesgos que introducen los procedimientos automatizados a la empresa y a los procedimientos de apoyo que se deseen cambiar, asegurarse de que la solución propuesta funcione, que se hayan especificado los requerimientos de seguridad, y que estos sean compatibles con los sistemas en funcionamiento. Procure verificar la confiabilidad de la tecnología o servicio de seguridad mediante referencias, accesoria externa, garantías contractuales, etcétera.
11) Asegúrese de que la infraestructura tecnológica pueda soportar prácticas de seguridad automatizadas.

12) Piense en que requerimientos adicionales de seguridad se necesitan para proteger la infraestructura tecnológica.
13) Identificar y revisar las fuentes que permiten mantenerse al día con las reparaciones que mejoran la seguridad e instale las que sean apropiadas para su infraestructura.
14) Asegúrese de que el personal sepa cómo se integra la seguridad a los procesos usados diariamente. Documente los procesos y capacite al personal.
15) Pruebe los sistemas y los cambios mayores comparándolos con los requerimientos de operación y de seguridad en un ambiente que sea representativo para que los resultados sean confiables. Considere probar cómo se integran las funciones de seguridad con los sistemas existentes. No haga pruebas con los sistemas que estén en producción.
16) Lleve a cabo la aceptación final de los sistemas de seguridad comparando los resultados de las pruebas con los objetivos de la empresa y con los requisitos de seguridad que involucren al personal clave que los usarán, los ejecutarán y les darán mantenimiento.
17) Evalúe todos los cambios, incluyendo las reparaciones, para conocer el impacto que tendrán en la integridad, confidencialidad y pérdida de datos importantes, la disponibilidad de los servicios críticos, y la validez de las transacciones importantes. Sobre la base de este impacto realice pruebas antes de hacer los cambios.
18) Tome nota y autorice todos los cambios, incluyendo las reparaciones (para las reparaciones de emergencias es aceptable hacer el registro ex post facto).
19) Asegúrese de que la administración establezca los requisitos de seguridad y que revise con regularidad el cumplimiento de convenios internos de calidad de servicio así como los contratos con proveedores de servicios.
20) Analice la competencia profesional de los terceros que intervengan en sus operaciones y asegúrese que tengan los medios necesarios para estar en

contacto con la autoridad para actuar sobre los requerimientos y preocupaciones de seguridad de la empresa.

21) Analice la dependencia en el trabajo de terceros de los requerimientos de seguridad y mitigue los riesgos de continuidad, confidencialidad y propiedad intelectual mediante contratos, depósitos, penas y premios.

22) Identifique las funciones e información empresariales criticas y los recursos que son necesarios para soportarlas (aplicaciones, servicios de terceros proveedores y archivos de datos). Asegúrese de que estos medios de soporte estarán disponibles en caso de que ocurra algún incidente de seguridad para mantener la continuidad de las actividades. Asegúrese de que se identifiquen y resuelvan a tiempo los incidentes importantes.

23) Establezca los principios básicos para salvaguardar y reconstruir los servicios de tecnologías de la información, incluyendo alternativas a los procedimientos, a la provisión de insumos y servicios en casos de emergencia, a cómo regresar a las operaciones normales después de un incidente y cómo avisarle a sus proveedores y clientes.

24) En colaboración con los empleados clave, defina lo que se debe respaldar y guardar fuera del sitio para garantizar la recuperación de las actividades. Por ejemplo, datos críticos, documentación básica y otros recursos de la tecnología de la información. Verifique con regularidad que los recursos respaldados se puedan usar y estén completos.

25) Implante reglas de control de acceso a los servicios basadas en la necesidad de cada individuo de leer, añadir, cambiar o borrar información y transacciones. Considere con cuidado los derechos de acceso de los proveedores de bienes y servicios y de los clientes.

26) Asegúrese de que se ha asignado la responsabilidad de administrar las cuentas de los usuarios y los objetos de autenticación (contraseñas, tarjetas y otros dispositivos) que sirvan para controlar dispositivos de alto valor. Revise periódicamente las acciones y la autoridad de los administradores de cuentas.

Asegúrese de que la administración de cuentas y la de dispositivos no recaigan en la misma persona.

27) Detecte y anote las violaciones de seguridad importantes. Por ejemplo, accesos a sistemas y redes, aparición de virus, mal uso de recursos o programas ilegales. Asegúrese de que estas violaciones se reporten de inmediato y se resuelvan lo más pronto posible.

28) Para garantizar que terceras partes sean confiables y que las transacciones sean auténticas al emplear sistemas transaccionales computarizados, las instrucciones deben ser claras, adecuadas y que cumplan con las obligaciones contractuales.

29) Vigile que en todos los sistemas se usen programas de protección contra virus manteniendo al día las definiciones de los virus. Use sólo programas legalmente adquiridos.

30) Establezca una política formal sobre qué información puede entrar a la organización cuál puede salir. Configure los sistemas de seguridad de las redes, por ejemplo, cortafuegos, para que sigan estas políticas. Piense cómo se pueden proteger los dispositivos de almacenamiento transportables. Vigile las excepciones y actúe cuando ocurra un incidente.

31) Mantenga al día un inventario completo del equipo y los programas que se usen, y de sus configuraciones.

32) Revise con regularidad que todos los equipos y programas que están instalados estén autorizados y que se tengan las licencias apropiadas.

33) Use diversos controles sobre los datos para verificar su integridad (precisión, completes y validez) durante la entrada, proceso, almacenamiento y salida. Controle las transacciones para garantizar su autenticidad y que no puedan ser repudiadas.

34) Entregue material sensible sólo a quien esté debidamente autorizado para recibirlo.

35) Defina los tiempos de retención, de archivamiento y de almacenamiento para documentos de entrada y de salida, datos y programas. Asegúrese de que se cumplan los requerimientos de los usuarios y los requerimientos legales. En los datos y programas almacenados verifique frecuentemente su integridad y que los datos no puedan ser extraídos impropiamente.
36) Implante sistemas de seguridad física a las instalaciones de tecnologías de la información, especialmente en aquellas que están más expuestas a riesgos. Si puede obtenga asesoría de expertos.
37) Proteja las redes y el equipo de almacenamiento (particularmente el móvil) de daños físicos, robos, accedentes e intercepción).
38) El personal clave debe regularidad:
    a) Validar que lo controles de seguridad sean adecuados comparándolos con los requerimientos que se han definido a la luz de las vulnerabilidades actuales.
    b) Revise que excepciones de seguridad deben ser vigiladas continuamente
    c) Evalúe cómo funcionan los mecanismos de seguridad e identifique debilidades tales como detección de intrusos, pruebas de penetración y esfuerzo, y planes de contingencia.
    d) Que se actúe ante todas las excepciones
    e) Que vigile el cumplimiento de los principales controles.
39) Obtenga, cuando sea necesario, recursos externos competentes para revisar la seguridad de la información, los mecanismos de control, el cumplimiento de leyes, reglamentos y obligaciones contractuales relacionadas con la seguridad. Aproveche el conocimiento de los expertos internamente.

Adicional a lo anterior, dentro de los parámetros que se han descrito y que se consideran como los de mayor significación en materia de seguridad de información y de tecnología, se han abordado los elementos que en la práctica,

orientan los análisis de todo aquello que se reconoce y precisa como riesgos, tal como lo detallamos en las siguientes líneas:

2.4.4. Análisis de riesgos

La meta del análisis de riesgos es ayudar en la selección de salvaguardas costo-efectivas. Para Rita Summers[77], el análisis de riesgo incluye un estimado de las pérdidas potenciales y qué salvaguardas pueden reducirlas para identificar cuáles de entre estas salvaguardas son las mejores en función de su costo.

Definiciones:

- **Amenaza:** Un evento con el potencial de causar un acceso no autorizado, modificación, revelación o destrucción de información, aplicaciones, sistemas, servicios o procesos.
- **Vulnerabilidad:** Debilidad, defecto o falla
- **Riesgo:** El riesgo puede ser definido como “algo que puede causar un daño”, o como lo define.
- **Control, salvaguarda o mecanismo:** Medida de protección (técnica o normativa) de los activos informáticos.
- **Activo informático:** Puede ser datos, información, sistema, software, hardware, o cualquier elemento de tecnología de información.
- **Proceso crítico:** Todo proceso que impacte directamente en la consecución de los objetivos de la organización.

Clasificación de amenazas:

- Naturales
    - Fuego, inundación, terremotos, etcétera
- Humanas

[77] SUMMERS, Rita C. Secure Computing: Threats and Safeguards. USA:Mc.Graw Hill.1996. p.1-11

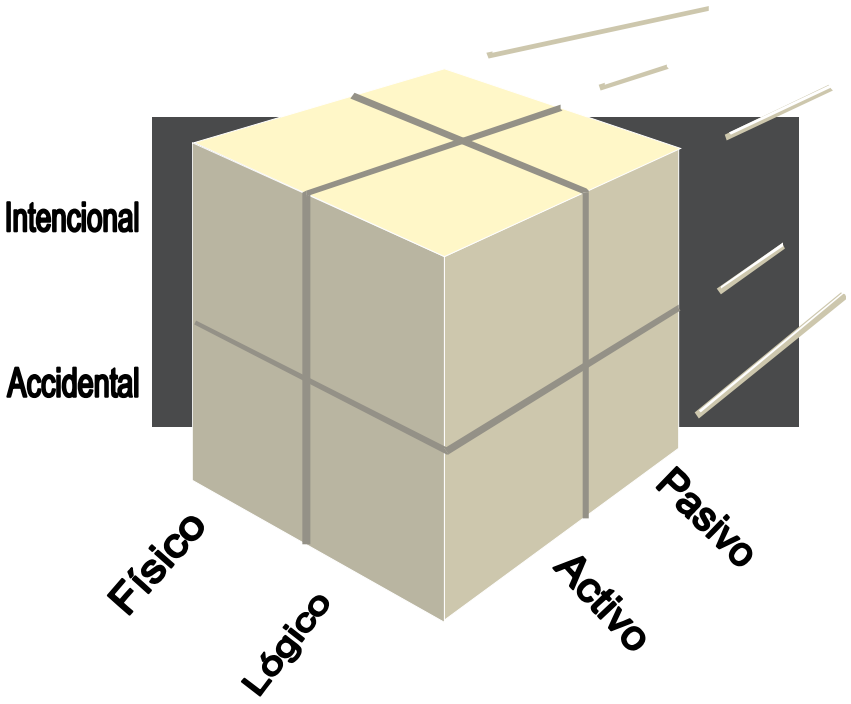
- Accidentales

  Negligencia, ignorancia
- Intencionales

  Vandalismo, espionaje, guerra electrónica, etcétera

Una forma ordenada para clasificarlas puede ser:

Gráfico 1. Cuadro de clasificación de amenazas



Ejemplos:

- Intencional, activo, físico: robo
- Intencional, activo, lógico: acceso no autorizado
- Intencional, pasivo, físico: duplicado de llaves
- Intencional, pasivo, lógico: escucha del teclado
- Accidental, activo, físico: inundación, temblor
- Accidental, activo, lógico: velado accidental de microficha
- Accidental, pasivo, físico: envío equivocado de llaves
- Accidental, pasivo, lógico: envío equivocado de fax

Estas categorías, además de ser de ayuda en la enumeración de amenazas, sirven también para buscar algunas soluciones genéricas para reducir grupos de amenazas con una sola acción. Por ejemplo, un estricto procedimiento de control de acceso físico puede reducir al mismo tiempo riesgos intencionales activos y pasivos físicos.

Análisis de riesgos informáticos

- Es parte fundamental en la administración de la seguridad
- Entre los beneficios que genera:
  - Identifica los puntos más débiles de la infraestructura de TI que da soporte a los procesos críticos de la organización
  - Guía la selección de medidas de protección de costo adecuado
  - Determina dónde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio
  - Permite realizar políticas de seguridad mejor adaptadas a las necesidades de la organización

Vulnerabilidades:

Considerando que la definición de vulnerabilidad en este contexto es la ausencia o debilidad de una salvaguarda que mitiga un riesgo, lo cual es una condición que tiene el potencial de aumentar la frecuencia de ocurrencia, el impacto o factor de exposición, o ambos, del riesgo. El análisis consiste en la identificación de estas ausencias o debilidades.

La mejor forma de llevarlo a cabo es a través de entrevistas individuales estructuradas con quienes tienen la responsabilidad de implementar las políticas institucionales mediante medidas administrativas o medidas de control. En las entrevistas hay que reducir la subjetividad y aumentar la consistencia y

profundidad de las preguntas. Hay que emplear una serie predeterminada de preguntas que hagan evidentes las posibles fallas en la implementación de mecanismos de defensa.

Se deben analizar los mecanismos que están presentes desde el punto de vista de cada una de las componentes de los activos, precisando qué conceptos se emplearon para proponer un mecanismo para proteger un activo dado. En cada caso debe estimarse el factor de exposición, o sea, qué porcentaje del valor del activo puede perderse si se materializa un riesgo antes y después de la implantación del mecanismo en cuestión.

Hay que asociar de la manera más explícita posible las vulnerabilidades con las amenazas a los activos para entender su interrelación. Este es uno de los conceptos fundamentales del análisis de riesgos. Si no se realiza este mapeo explícitamente, resulta difícil establecer las ramificaciones o consecuencias de una vulnerabilidad. La relación puede ser intuitivamente clara, pero debe permitir el uso de alguna métrica para que sea posible llevar a cabo un análisis de costo/beneficio.

Tipos de análisis de riesgos:

- **Cuantitativo**
    - Enfocado a determinar valores numéricos (generalmente monetarios) a los componentes objeto del análisis, así como al nivel de posibles pérdidas.
    - Los resultados son objetivos, basado en métricas generadas igualmente de forma objetiva. Estos se expresan en porcentajes, probabilidades de ocurrencia de amenazas, pesos, etcétera.
    - Es sencillo mostrar el costo-beneficio en términos comprensibles a la alta dirección (no técnicos)

- Los cálculos pueden resultar complejos
- El trabajo previo requiere tiempo y esfuerzos considerables

- **Cualitativo**
  - No requiere determinar valores numéricos (generalmente monetarios) a los componentes objeto del análisis, así como el nivel de posibles pérdidas.
  - No es necesario contar con la frecuencia de ocurrencia de las amenazas
  - Los resultados son subjetivos
  - No hay una base para demostrar el costo-beneficio
  - Los cálculos son sencillos
  - La calidad del análisis depende del equipo conformado

Las siguientes preguntas pueden presentarse durante el proceso de análisis de riesgos:

- ¿Qué puede suceder? (amenaza)
- Si sucede, ¿qué tanto daño causará? (impacto)
- ¿Cada cuándo sucederá? (Frecuencia, anualizada)
- ¿Estamos seguros de lo anterior? (incertidumbre)
- ¿Qué puedo hacer? (mitigación)
- ¿Cuánto va a costar? (anualizado, e incluso multi-anualizado)
- ¿Vale la pena hacerlo? (costo/beneficio)

El proceso de análisis de riesgos tiene varias de las fases siguientes, dependiendo de si éste se realizará de manera cuantitativa o cualitativa:

- Identificación de los activos (ambos)
- Valoración de los activos (cuantitativo)
- Identificación de las amenazas (ambos)

- Análisis de vulnerabilidad (ambos, implícito en el análisis del impacto a la organización)
- Análisis del impacto estimado a la organización (ambos)
- Identificación de los mecanismos de reducción de vulnerabilidades (ambos)
- Valoración de los mecanismos (ambos)
- Análisis del beneficio logrado con el costo estimado (ambos)

Durante el proceso de análisis deben contestarse las siguientes preguntas:

- ¿Qué es un riesgo para la organización? Básicamente, cómo pueden verse afectados los procesos de misión critica de la organización
- ¿Qué impacto tiene la materialización de un riesgo en las metas de la organización?
- ¿Qué riesgos son aceptables?
- ¿Cuál es la dependencia de la organización en las tecnologías de información, y los recursos informáticos manejados en ella?
- ¿Qué medidas de defensa existen para eliminar los riesgos no aceptables y cuánto cuestan?
- ¿Qué medidas de protección resultan en el mejor beneficio por el costo?
- ¿Quién se responsabiliza de las medidas de protección?
- ¿Cómo y cuándo se implementarán esas medidas de protección?

Análisis de riesgos cualitativo

Metodología para un análisis de riesgos cualitativo[78]

Debido a que el análisis de riesgos es un proceso continuo y dado que los sistemas, datos y procedimientos cambian día con día en las organizaciones, los

[78] PELTIER, Thomas R. *Information Security Risk Analysis*. USA: Auerbach. 2005. 296 p. ISBN-10: 0849308801.

métodos cualitativos para estimar el riesgo han cobrado en las últimas fechas buena aceptación.

A continuación se describen 10 pasos a seguir para realizar este análisis en unas cuantas semanas.

Estudio inicial

- Debe identificarse amenazas, vulnerabilidad y medidas de protección para reducir el impacto de que una amenaza se concretice.
- Antes de desarrollar la política de seguridad, deben ser identificados los activos informáticos, las principales amenazas, evaluar el riesgo, realizar un estudio costo-beneficio e implantar los mecanismos que permitirán reducir los riesgos.

Identificación de los activos

- Antes de iniciar el análisis se debe identificar la lista de activos que deben ser protegidos, así como la dependencia entre ellos.
- Esta lista debe ser regularmente actualizada (con la llegada de nuevo equipo, cambios de infraestructura, etcétera.
- Entre otras cosas se debe considerar: hardware, software, datos, documentación, servicios u operación.

Esta etapa normalmente se cumple mediante un análisis de la misión de seguridad que establezcan los dueños de la información, pues a partir de ésta se puede derivar qué es lo que se desea proteger. Sin embargo, este análisis puede ser complicado, pues los sistemas de información cada día son más complejos. El uso de las redes de computadoras, particularmente en forma de intranets y extranets, y los procesos de adquisición, fusión y fragmentación de organizaciones, frecuentemente resultan en la inexistencia de un inventario completo de los bienes informáticos de una organización. Además, la proliferación de la información

interna disponible a los miembros de una organización dificulta aún más la realización de inventarios completos.

En términos generales, una metodología práctica es establecer perímetros que se puedan definir bien y llevar a cabo el inventario dentro de esos perímetros. Posiblemente el único análisis de riesgos factible será el que se haga perímetro por perímetro.

La temporalidad es un factor determinante en el análisis de riesgos. La vida útil de los equipos, de los programas, de los datos y de los mecanismos de protección, dominan el estudio de los beneficios y de los costos. Por ejemplo, un mecanismo de protección cuya vida útil es mucho más corta que la del sistema de información que está protegiendo, deberá ser reemplazado varias veces, y el costo por lo tanto no es sólo el del mecanismo inicial. Otro ejemplo puede ser el uso de la criptografía para proteger datos: si la vida útil de los datos es corta se puede emplear criptografía más débil (o sea más barata).

Otro factor temporal está indicado por la variación en el tiempo del valor de la información. Si sólo se considera el valor actual en el análisis de costo/beneficio, olvidando por ejemplo que la información no tendrá valor después de un período dado, se puede sobreestimar el beneficio que ofrece un mecanismo de protección. Por esto, el trabajo de análisis normalmente se hace sobre la base de cifras anuales. También se pueden emplear categorías generales predeterminadas como las que aparecen en el RFC 2196:

- **Equipo:** Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, unidades de disco, líneas de comunicación, servidores de terminales, ruteadores.

- **Programas:** Programas fuente, programas objeto, utilerías, programas de diagnostico, sistemas operativos, programas de comunicaciones.
- **Datos:** Durante la ejecución de programas, almacenados en líneas, archivados fuera de línea, respaldos, bitácoras para auditoria, bases de datos, datos en tránsito sobre medios de comunicación.
- **Gente:** Usuarios, administradores, personal de soporte y mantenimiento
- **Documentación:** De programas, de equipos, procedimientos administrativos locales.
- **Proveedores:** De papel, formas, cintas de impresora, medios magnéticos.

Usando estas categorías, para cada miembro de una de ellas se pueden anotar las amenazas que se aprecian o se conocen.

Entrevistas

- Para definir la importancia de un cierto activo, así como el riesgo asociado a éste, es necesario contar con el apoyo de las áreas que crean, procesan o administran la información.
- Este apoyo es necesario concertarlo a través de varias entrevistas.

Los 10 pasos de la metodología:

1. **Enunciar el alcance**
    - Establece cuál es el activo informático a ser evaluado
        - Centro de computo
        - Sistemas: Unix, Windows, etcétera
        - Aplicaciones, BD
        - Wan, Land o redes críticas
    - Mantiene el enfoque en los procesos críticos de la organización
    - Define cuál será el entregable (reporte, estrategia, mecanismo, etcétera.

2. **Conformar el equipo de desarrollo del análisis de riesgos**
    - Dueños de las funcionalidad
    - Usuarios a todos los niveles
    - Diseñadores y analistas de sistemas
    - Desarrolladores de sistema
    - Administradores de BD
    - Auditores
    - Personal de:
        - Seguridad física
        - Telecomunicaciones
        - Jurídico
        - Administración de operaciones
        - Sistemas operativos
        - Seguridad informática

3. **Identificar las amenazas**

    La primera etapa del proceso de análisis de riesgos consiste en hacer una enumeración de las amenazas que pueden afectar a los activos informáticos. Esta lista varía de caso en caso, pero se pueden adoptar algunas técnicas para proceder a elaborar la lista en forma ordenada.

    Un concepto que es importante es el de desagregación.

    Es recomendable contar con una lista propuesta antes del análisis. Pero fomentar lluvias de ideas:

    - Lectura ilegal de información
    - Negación de servicio
    - Explotación de deficiencias en plataformas operativas
    - Vandalismo en páginas Web
    - Falsificación de identidad

- Virus, caballos de Troya, gusanos
- Ingeniería social
- Acceso no autorizado
- Corrupción de datos
- Instalaciones deficientes
- Controles de acceso físico débiles
- Protecciones físicas no consideradas
- *Spyware*
- *Phishing*
- Consultar publicaciones internacionales CSI/FBI (www.gocsi.com)

Espionaje industrial

Información que buscan obtener los competidores en un espionaje industrial:

- Precios
- Procesos de fabricación
- Desarrollo de productos
- Listas de clientes
- Investigación básica
- Código fuente
- Información de ventas
- Información personal
- Información de costos
- Información de propuestas
- Planes estratégicos

Código mal intencionado

- Virus
- Gusanos

- Caballos de Troya
- Bombas lógicas
- Sistemas de explotación de canales encubiertos
- Causan enormes costos en la identificación y eliminación, así como en tiempo muerto

Tempest (Transient Electromagnetic Pulse Emanation Standard)

- Se estima que la industria *Tempest* sobrepasa el billón de dólares al año en negocios (para bien y para mal)
- Esto nos hace pensar que existe una verdadera amenaza a combatir

Canales encubiertos

- Canal por el que se puede filtrar información sin pasar por los controles impuestos por un monitor de referencia
- Su grado de peligrosidad está en función del ancho de banda con que cuenten para sustraer información confidencial
- En un sistema operativo puede haber cientos de estos canales

Ingeniería social

- Recoger papeles de los cestos de basura
- Llamar al personal haciéndose pasar por soporte técnico.
- "Conquistar" a alguien dentro de la organización
- Disfrazarse de personal de intendencia, vigilancia, etcétera.
- Ampliamente usados en virus actuales

Hay que tratar de analizar todas las amenazas por separado, aunque esto es difícil. Si no es posible, hay que buscar grupos que tengan elementos comunes. Esto facilita el análisis de mecanismos de protección y el consiguiente estudio de costos.

4. Priorizar las amenazas

- Tabla para dar prioridades a las amenazas (por consenso). Esta mismo tabla se emplea para determinar el impacto a la organización

Tabla 8. Tabla para dar prioridades a las amenazas

Baja	Baja a Media	Media	Media a Alta	Alta
1	2	3	4	5

Tabla 9. Hoja de factor de riesgo

Hoja de factor de riesgo

Amenaza	Posibilidad de ocurrencia (prioridad de la amenaza)	Impacto a la Organización	Factor de riesgo total estimado

5. **Determinar la prioridad en función del impacto**
    - Se realiza el análisis del impacto que provocaría la ocurrencia de incidentes provocados por las amenazas identificadas
    - Este análisis se realiza amenaza por amenaza
    - Inicialmente se puede suponer que no se cuenta con controles para mitigar el impacto
    - Más adelante se permitirá reconsiderar los controles existentes y cómo mitigan el impacto estimado.

6. **Estimar el impacto total de la amenaza**
    - Simplemente se suman las columnas de prioridad de que ocurra la amenaza y la del impacto a la organización, para obtener un valor entre 2 y 10 del factor de riesgo total estimado.
    - Las amenazas que tengan un factor de riesgo igual o superior a 6 serán reconsideradas cuando se pase a la etapa de selección de los controles necesarios

7. **Identificar medidas de protección**
    - Se busca encontrar con controles técnicos, administrativos, legales, físicos, para proteger con un costo razonable a los activos, conforme a las amenazas de mayor factor de riesgo.
    - Los controles se clasifican en:
        - Preventivos (para evitar eventos que se supone pueden ocurrir)
        - De detección (para detectar eventos con la suficiente anticipación para tomar una medida)
        - De recuperación (para planear y responder tan rápido como sea posible ante un evento y establecer un ambiente de operación segura)

- De garantía (para asegurar que los controles implantados son efectivos).

- Ejemplos de los controles:
  - Preventivos (cifrado, control de acceso, análisis de riesgos, políticas)
  - De detección (IDS, IPS, Anti-código malicioso, CCTV)
  - De recuperación (BCP, BIA, DRP)
  - De garantía (Pentest, monitoreo periódico, revisión de seguridad de aplicaciones, apego a estándares, auditorías de seguridad)
- Se debe asociar a cada amenaza uno o varios controles, así como su costo

Una herramienta de ayuda pueden ser los controles que publica en su reporte anual el CSI/FBI:

Tabla 10. Controles del CSI/FBI

Amenaza	Factor de riesgo total estimado	Posible control (solución)	Costo del control

8. Realizar un análisis costo/beneficio

- Se debe vigilar que los controles seleccionados siguen los objetivos de la organización
- En este análisis, se debe determinar cuáles son los controles que dan un máximo de protección, a un menor costo (puede haber controles que sirvan para mitigar la ocurrencia de varias amenazas)

- Asimismo, debe pensarse en las implicaciones que tendrá la implantación del control en la organización (administración, capacitación, cultura organizacional, etcétera.

9. Ordenar las medidas de protección por prioridades

- Debe ordenarse la selección para elegir el control adecuado
- Elementos que influyen son:
    - Cuántas amenazas puede mitigar un control
    - El impacto en la productividad al implantar un control
    - Controles que pueden desarrollarse en casa
    - Nivel de aceptación de riesgo

10. Reportar el resultado del análisis

- El producto del análisis es un reporte donde se documentan los hallazgos
- Puede en ocasiones llegar hasta esbozar un plan de implantación de los controles sugeridos.
- Permite crear un histórico, que permitirá apoyar las decisiones en análisis futuros
- Los puntos que debe incluir el reporte en:
    - Introducción
    - Antecedentes y alcance del análisis
    - Resumen ejecutivo
    - Identificación de amenazas
    - Determinación del factor de riesgo total
    - Identificación de controles
    - Análisis costo-beneficio
    - Recomendación de controles
    - Anexos
    - Miembros del equipo

- Glosarios
- Referencias
- Planes de implantación recomendados
- Control de cambios

El modelo de seguridad debe estar basado en las políticas que la organización ha determinado como parte de su operación. Las políticas que se definen deben ser periódicamente revisadas y actualizadas, debidamente divulgadas para garantizar el conocimiento de ellas por parte de todos los miembros de la organización, apoyo total de la administración, suficientes recursos para la implementación y un equipo de personas dedicadas a esta función, son aspectos básicos para lograr los objetivos buscados. La seguridad de TI no es un proyecto que logre desarrollarse de manera inmediata o de una vez, es un campo que requiere investigación permanente, actitud proactiva y generar una cultura organizacional que propenda por la seguridad como parte de la función de la organización, que no es otra cosa que tener presente de manera constante que la seguridad tiene un costo, pero la inseguridad tiene un costo mayor.

¿Qué tecnología se debe desarrollar para garantizar la seguridad del futuro inmediato?

- Seguridad de acceso a nivel del sistema operativo.
- La encriptación y la firma electrónica ante la posibilidad de interceptaciones de información en la red.
- La biometría (lectores de retina, huellas digitales, etc.). Aunque ya existen manuales de cómo violar éstas seguridades.
- Sistemas de comunicación sin cables.

¿Qué recomendaciones personales deben ser tenidas en cuenta?

- Establecer políticas de seguridad en las empresas, no sólo a través de cortafuegos (*firewalls*) en Internet, sino también dentro de sus redes privadas.
- Claves diferentes para los distintos sitios a que tenga acceso.
- Consejos para claves o contraseñas: use combinaciones alfanuméricas, mayúsculas y minúsculas, no use palabras, ni secuencias de letras o números, no use fechas de nacimiento, números de sus tarjetas, que su clave no sea el mismo nombre de usuario y use por lo menos 8 caracteres.
- Cambiar periódicamente su clave
- No permitir accesos simultáneos con el mismo login.
- Bloqueo de cuenta luego de tres intentos fallidos al digitar la clave.
- Para sus programas de correo o el acceso a otros sitios, generalmente es posible permitir que Windows automáticamente recuerde la clave, sin que sea necesario que usted la digite, esto permite que cualquier usuario en su maquina entre con sólo tener su *login*. Evite esto.
- Los *passwords* son claves de seguridad, por lo tanto deben ser sólo de su conocimiento.
- No conectarse a Internet directamente a través de la red local.
- Emplear un sistema operativo de red lo más seguro posible, aprovechando las herramientas que provee.
- Dar a conocer a los usuarios de la empresa los riesgos y mecanismos que usan, para que por inocencia o desconocimiento no sirvan en bandeja de plata la seguridad de la organización a otros. Hay que evitar hacer atractiva la empresa para los intrépidos *crackers* u otros. Ver Anexo 1.
- No entregar información personal, a menos que sea necesario.
- Borrar los rastros y las galletitas (lo puede hacer utilizando un editor de texto), pero recuerde que esto hará más lento su trasegar por aquellos sitios.
- Es necesario revisar con frecuencia el registro de ingresos (*logs*).

En este orden de ideas, y apoyados en los referentes desarrollados expondremos a continuación los elementos considerados a la hora de revertir nuestra propuesta en el desarrollo de un modelo de seguridad de TI, basados en la prueba empírica de la encuesta que aplicamos y que, adicionalmente se estructuró siguiendo las líneas de la bibliografía secundaria en lo relativo a los puntos, lógica interna y estrategias de seguridad y de evaluación de tecnología implementadas en los Estados Unidos y Europa.

2.5. MODELO DE SEGURIDAD DE TECNOLOGÍA DE INFORMACION (TI)

Para nuestra propuesta del modelo de seguridad de TI hemos seguido contextualmente la propuesta desarrollada Daltabuit, Enrique; Hernández, Leobardo, Mallen, Guillermo y Vásquez, José.[79] Como bibliografía de apoyo puede consultarse la siguiente: Integración de un Sistema de gestión de seguridad de la información con un Sistema de Gestión de la Calidad de Andrea Marcela Barrientos Arcila y Alexandra Areiza Córdoba[80]; Hacia un Modelo de Madurez para la seguridad de la información de Juan Guillermo Lalinde Pulido y Otros[81] y Los Criterios comunes sobre evaluación de la confiabilidad de tecnologías de la información de Jaquelina López[82].

---

[79] DALTABUIT, Enrique; HERNÁNDEZ, Leobardo; MALLEN, Guillermo; VÁSQUEZ, José., Op.Cit., 774p.

[80] BARRIENTOS ARCILA, Andrea Marcela; AREIZA CÓRDOBA, Alexandra. Integración de un Sistema de gestión de seguridad de la información con un Sistema de Gestión de la Calidad. Medellín: Universidad Eafit. 2005.

[81] LALINDE PULIDO, Juan Guillermo y Otros. Hacia un Modelo de Madurez para la seguridad de la información. Medellín: Universidad Eafit. 2005.

[82] LÓPEZ, Jaquelina. Los Criterios comunes sobre evaluación de la confiabilidad de tecnologías de la información. México: Universidad Nacional Autónoma de México. 2001.

“Las buenas prácticas de administración indican que la existencia de un enunciado público claro sobre la misión de una organización es indispensable para que todos los miembros ubiquen sus propios esfuerzos. Se evitan confusiones y alegatos, se fomenta la productividad y se logra un mejor ambiente de trabajo.”[83] Además, permite elaborar políticas operativas que facilitan cumplir la misión de la organización, que deben entenderse como reglas que hay que seguir obligatoriamente.

“Normalmente se enuncian en forma positiva, es decir, indican qué debe hacerse y, en ocasiones, cómo. Pero también, a veces en forma negativa, como prohibiciones. Las políticas eventualmente se implementan mediante procedimientos detallados.”[84]

2.5.1. Misión de seguridad

Concebir y redactar la misión y las políticas de una organización recae sobre los responsables del buen funcionamiento de la misma. Por ejemplo, los dueños de una empresa, los principales administradores de una corporación o los directores de alguna dependencia. El elemento fundamental de estos documentos es que expresan el consenso de quienes conocen mejor que nadie los principios operativos, económicos y éticos que conducirán al éxito colectivo.

---

[83] JAUCH, Lawrence R.; GLUECK, William F. Business Policy and Strategic Management. USA: McGraw-Hill Companies. 1988. 960 p. ISBN-10: 0071005072.

[84] ABRAHAMS, Jeffrey. The Mission Stament Book: 301 Corporate Staments from America´s Top Companies. USA: Ten Speed Press. 1996. 512 p. ISBN-10: 1580081320

CARVER, John. CarverGuide, Creating a Mission That Makes a Difference. New York: Jossey-Bass. 1996. 24 p. ISBN-10: 0787903027

Al hacer este trabajo es necesario consultar los expertos en diversos tipos de actividad para que los directivos sepan cómo afectarán las políticas que emitan la capacidad de acción de las diferentes secciones de la organización. La forma más eficiente de realizar esta consulta es mediante una encuesta preparada por expertos en seguridad informática que planteen las preguntas en forma tal que conduzcan a párrafos precisos en la redacción de la misión, cada uno de los cuales pueda plasmarse en una o más políticas de seguridad.

Todas las disciplinas de seguridad (personal, física, informática, etc.) trabajan en forma conjunta para establecer una infraestructura de seguridad que sirva a toda la organización. Definen cuál es el comportamiento aceptable y cuáles son los riesgos aceptables, y determinan cómo mitigan los riesgos que no son aceptables aplicando garantías medibles que hacen manejables y aceptables los riesgos. Las palabras "medibles" y "aceptables" son fundamentales.

Garantías tales como cercas, la confiabilidad del personal o algoritmos de cifrados son herramientas importantes para controlar los riesgos en algunos entornos. "Medir la efectividad de la cerca para evitar intrusos (puede leerse, igualmente, como Muro de Contención), la confiabilidad de un empleado analizando su biografía para detectar si ha cometido fraudes o medir un servicio de cifrado para saber hasta qué grado ofrece confidencialidad de la información es básico para poder tomar decisiones sobre qué riesgos son aceptables"[85]

Los que se dedican a la seguridad informática agrupados en el SANS[86] consideran que los errores más frecuentes que cometen los directivos son:

---

[85] FERRIS, J. M. Using Standards As A Security Policy Tool. In: StandartView. New York: ACM Press. Volume 2, Issue 2. June, 1994. p. 72-77. ISSN:1067-9936.

[86] GUEL, Michele D. A Short Primer for Developing Security Policies. En: SANS Institute. 2007. 43 p. <http://www.sans.org/security-resources/policies/Policy_Primer.pdf>. [citado en Mayo 1 de 2009]

1. Suponer que los problemas desaparecerán si no se le hace caso.
2. Autorizar soluciones reactivas y parches de corto plazo tales que los problemas reaparecen rápidamente.
3. No entender cuánto dinero vale la información y qué tanto depende de ella la reputación corporativa.
4. Depender principalmente de un cortafuegos.
5. No lidiar con los aspectos operacionales de la seguridad.
6. Hacer sólo unos cuantos parches y no dar seguimiento para estar seguros de que los problemas en verdad estén resueltos.
7. No entender la relación que existen entre la seguridad y los problemas de funcionamiento.
8. Entienden la física pero no ven las consecuencias y no las capacitan ni les dan tiempo para capacitarse.
9. Designan a personas no capacitadas para mantener la seguridad y no las capacitan ni les dan tiempo para capacitarse.

La solución de algunos de estos problemas consiste en:

- Ubicar la seguridad informática al mismo nivel que otras actividades sustantivas de la organización.
- Elaborar la misión de la seguridad informática claramente
- Promulgar las políticas que se derivan de la misión
- Determinar qué mecanismos se requieren para implementar esas políticas.

2.5.2. Consenso

El método para llegar a un consenso en estas políticas de tipo general es parlamentario, e involucra a decenas de personas con representación de la comunidad, que cuenta con personal de apoyo especializado.

No existe una fórmula para encontrar las mejores palabras que expresen la intención colectiva de una organización. La puede redactar una persona sola o

después de una sesión colectiva de intercambio de opiniones. Lo más importante es que se logre un consenso en las respuestas a las preguntas que se usan para elaborar la misión.

> "Otro enfoque es emplear tiempo de los directivos en un retiro para discutir las preguntas buscando temas en los que exista consenso. Puede ser útil inmediatamente después discutir el texto de la misión. Durante la discusión aparecen sutilezas, cambios en el entorno y los participantes más experimentados compartes sus puntos de vista con los más inexpertos. De esta forma el grupo directivo adquiere confianza de que la misión que resulte representa verdaderamente las ideas comunes."[87]

Estos retiros pueden tender a discusiones poco productivas. Hay que usar técnicas efectivas en la obtención de consenso sin permitir discusiones estériles. Una forma de hacerlo es usar el método Delphi.

2.5.3. El método Delphi

Un mecanismo para explorar vías hacia el consenso que se emplea rutinariamente en cuerpos colegiados y legislativos locales es el método Delphi que consiste en términos generales de rondas de preguntas o propuestas presentadas al cuerpo deliberativo en forma tal que sus respuestas no se puedan discutir abiertamente, solamente en forma acotada y encauzada.

En 1936, Douglas Mac Gregor afirma que las predicciones hechas por un grupo son más acertadas que las que hacen sus miembros individualmente. Las

---

[87] POLYCASTRO, Michael. Introduction to strategic planning: Management and planning series. En: U.S. Small Bussines Administration. 2004. 17 p. <http://www.sba.gov/idc/groups/public/documents/sba.../pub_**mp21**.pdf> [citado en 20 de abril de 2009]

discusiones colectivas tienden a ser dominadas por uno o dos individuos y tienden a apegarse a una sola idea durante periodos largos. La técnica Delphi es una respuesta a estas observaciones.

La primera aplicación fue en 1948 para tratar de mejorar el resultado de apuestas en carreras de caballos. Su verdadero origen en los cincuenta se debe a Olaf Helmer y Norman Dalkey de la Corporation RAND. Se emplea en una gran diversidad de situaciones.

Definición

Es un método para estructurar el proceso de comunicación de un grupo de personas para que funcionen efectivamente lidiando con problemas complejas. Los participantes, que son a menudo quieres esperan obtener el producto del ejercicio Delphi, son los que deciden. Se emplean moderadores: quienes diseñan los cuestionarios, resumen los resultados y conducen el proceso para satisfacer los requerimientos de quienes deciden. Se acude a expertos cuya opinión se necesita y a quienes se les hacen las preguntas.

Metodología

- Los moderadores preparan una serie de preguntas para los expertos. Se solicita y se evalúa su opinión sin que se comuniquen entre ellos.
- Se prepara una segunda serie de preguntas
- Se solicita y se evalúa su opinión sin que se comuniquen entre ellos y así sucesivamente hasta lograr consenso y encontrar bloques donde el consenso será disponible.

Características

Preguntas estructuradas: se usan cuestionarios escritos para mantener enfocado al grupo.

Iteración: se realizan rondas después de que se conozca el resultado de la primera. Permite a los moderadores controlar el proceso y canalizarlo hacia un producto compacto.
Retroalimentación controlada: dar al grupo las respuestas de todo el grupo para que reconsideren en lo individual su respuesta.
Anonimato de las respuestas: se logra recogiendo los cuestionarios lo cual permiten a los panelistas expresarse libremente sin sufrir las presiones de grupo directamente.

Procedimiento

La misión debe redactarse en varios párrafos, cada uno de los cuales contendrá una colección de conceptos relacionados, susceptibles de ser aprobados o rechazados conjuntamente.

Cada párrafo se escribe en una hoja de papel. Cada uno de los conceptos debe ser susceptible de plasmarse en una o más políticas de seguridad. Este material es preparado por los moderadores de la sesión Delphi con la ayuda de especialistas en seguridad informática que hayan tenido la oportunidad de estudiar la organización.

> *Sobre este particular pueden analizarse las propuestas metodológicas desarrolladas por la OCDE con relación a las técnicas para definir las estrategias de seguridad que a puntan a consolidar la seguridad de TI como una variable de la cultura organizacional. Organization for Economic-Operation and Development. organización para la cooperación y el desarrollo económicos. Ver Anexo 2*

Los participantes serán los miembros del organismo normativo. Cada participante anotará en su hoja un numero que indicará su total acuerdo (10) con el párrafo o su desacuerdo total (0), pudiéndose anotar un indicador de acuerdo parcial. Se

recogerían de inmediato las hojas mencionadas. Se repetirá este proceso para todos los párrafos que constituyen la misión.

Métrica

Para cada párrafo se calculará el promedio y dispersión de las medidas de aceptación:

- Los que obtengan una aceptación de 8 o mayor con una dispersión baja se consideran aprobados.
- Los que obtengan una aceptación de 2 o menor con una dispersión baja se consideran rechazados.
- Los que obtengan una aceptación entre 2.1 y 7.9, y los que tengan una aceptación con una dispersión alta se someten a una nueva evaluación.

Para cada párrafo a evaluar en la segunda ronda, se entrega a los participantes una hoja en la que aparezca el párrafo a evaluar y se invita a un voluntario a hablar a favor y a otro voluntario a hablar en contra. Al terminar los argumentos se procede a recoger las evaluaciones. Se repite el proceso con todos los demás párrafos de la segunda ronda.

Al terminar la segunda ronda se clasifican los párrafos como aceptados o rechazados. Los párrafos aprobados constituyen la misión de seguridad y dan origen a las políticas que deben adoptarse y a los mecanismos que se implanten.

Participantes

Los actores participantes en las políticas de seguridad y sus responsabilidades son:

- ***Alta administración***
    - Tiene la responsabilidad del éxito de la organización
    - Fija los objetivos, metas y prioridades para apoyar la misión de la organización

- Verifica que se asignen recursos adecuados al programa y que este se desarrolle con éxito.
- Da el ejemplo a los demás

- ***Dueños de programas, administradores de funciones, dueños de aplicaciones***
  - Aplican medidas de seguridad a sus áreas de responsabilidad
  - Aplican controles técnicos, administrativos y operativos.
  - Sus subordinados son los que hacen el verdadero trabajo directo.
- ***Administradores de la seguridad de sistemas de cómputo***
  - Guían la administración diaria del programa de seguridad en cómputo.
  - Coordinan las interacciones que involucran la seguridad de los diversos elementos externos de la organización.
  - Frecuentemente, si los programas, funciones o aplicaciones son grandes o complicadas, se asigna a cada una un oficial de seguridad.
- ***Administradores de configuraciones, proveedores de tecnología que***
  - Implementan la tecnología de seguridad diseñada para el sistema
  - Deben dar continuidad a sus servicios
  - Probablemente pertenezcan a una organización grande de administración de recursos de información
  - Pueden atender incidentes directamente
- ***Organizaciones de soporte***
  - Analizan la vulnerabilidad de los sistemas
  - Proveen los servicios de comunicación
  - Ayudan a los dueños y administradores a implantar y vigilar sistemas específicos para un programa o aplicación
  - Coordinan los sistemas de seguridad entre aplicaciones o programas
  - Auditores, especialistas en seguridad física, especialistas en planes de contingencia, especialistas en recuperación después de desastres, especialistas en calidad confiabilidad, departamento de adquisiciones y

soporte, departamento de capacitación, departamento de personal, especialistas en administración de riesgos, departamento de servicios generales, verificadores independientes, equipos de penetración independientes, usuarios de sistemas.

2.5.4. Políticas de seguridad

Una vez que se ha establecido la misión de seguridad informativa se requiere redactar las políticas en que se basara el cumplimiento de la misión. Hay que usar políticas de seguridad porque sin ellas no se tiene un marco de referencia general de seguridad, ya que definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los “dueños” y permiten adoptar una actitud de buen vecino en un entorno cada vez más globalizado.

Los elementos de un sistema de seguridad deben apoyar la misión de la organización y forman parte integral de una buena administración. El sistema debe tener un costo/beneficio bajo para que sea aceptable. Las tareas y la responsabilidad deben ser explícitas y se requiere un enfoque integrado y completo que debe ser revaluado periódicamente.
Los que administran sistemas tienen responsabilidad de seguridad que trascienden sus propias organizaciones. Además se enfrentan a factores sociales que deben tomarse en cuenta.

En este orden de ideas, se sugieren entonces, los referentes que en la práctica darán cuenta de la forma como se construye dicho modelo y, para ello, aplicamos una encuesta como soporte empírico para validar nuestra hipótesis de investigación que, luego de presentar la tabulación de la encuesta estaremos mostrando como producto final de este trabajo.

2.6. ENCUESTA

A continuación se presenta la encuesta realizada en las 20 empresas de Medellín, en donde se explora la cultura de seguridad de TI, en las mismas.

2.6.1. Modelo de encuesta

Nombre: _____ Cargo: _____

Empresa: _____ Fecha: _____

Gracias por participar en la encuesta sobre cultura organizacional y seguridad de tecnología informática, organizada por estudiantes del MBA de la Universidad EAFIT. Estamos muy interesados en su opinión y agradecemos sinceramente su participación en esta iniciativa. Los resultados de la encuesta permitirán conocer que tan arraigada se encuentra la **seguridad de tecnología informática (TI)** en su empresa y su relación con la **cultura organizacional**.

Todas las respuestas son de carácter confidencial y las respuestas individuales no serán reveladas. La información solo se utilizará en conjunto y agregada una vez compilada y analizada.

Entendemos por:

Cultura organizacional: La cultura es un conjunto de elementos, más o menos tangibles producidos y, sobre todo, poseídos por la organización. Dicho de otra

manera, la organización tiene una cultura al igual que posee una estructura o una tecnología. La cultura es una variable organizacional que moldea la identidad de la empresa.

Seguridad de tecnología de información (TI): La seguridad debe ser una consideración diaria, la seguridad debe ser un esfuerzo comunitario, las prácticas de seguridad deben mantener un foco generalizado, las prácticas de seguridad deben incluir medidas de entrenamiento para todo el personal de la organización y ser constitutivas de los principios rectores del clima, misión y visión organizacional, esto es, componente vital de la cultura organizacional.

Gracias por su tiempo.

Favor marcar con una X según corresponda.
Total No. preguntas: 26
Tiempo aproximado: 6.5 minutos

1. ¿Cuál es el sector primario de su empresa?
    - [ ] Servicios Financieros /Inversiones/Banca
    - [ ] Construcción/Ingeniería
    - [ ] Educación
    - [ ] Gobierno/Sector Público/Servicios Públicos
    - [ ] Seguros
    - [ ] Transporte
    - [ ] Tecnología / Telecomunicaciones
    - [ ] Manufactura/Industria/Alimentos
    - [ ] Otro, especifique: _____

2. ¿Cuántos empleados tiene su organización (Incluye temporales y subcontratados)? ¿Si su empresa es una multinacional, por favor indique los empleados en Colombia?

    [ ] Menos de 100
    [ ] De 101 a 500
    [ ] De 500 a 1000
    [ ] De 1000 a 2500
    [ ] Más de 2500

3. ¿Cuál es su cargo en la organización?

    [ ] Secretaria/Auxiliar
    [ ] Analista
    [ ] Jefe/Ejecutivo/Coordinador
    [ ] Director
    [ ] Gerente
    [ ] Otro, especifique cual: _____

4. ¿Cuál es área en la que se desempeña?

    [ ] Tecnología/Sistemas
    [ ] Administrativo
    [ ] Contraloría/Auditoria
    [ ] Ventas
    [ ] Mercadeo
    [ ] Producción
    [ ] Otro, especifique cual: _____

5. ¿Qué tan frecuentemente usa Internet para su trabajo?
    [ ] Constantemente
    [ ] Ocasionalmente
    [ ] Raramente
    [ ] Nunca

6. ¿Tiene la empresa en la cual trabaja una estrategia de **seguridad de TI**?
    [ ] Sí
    [ ] No

7. ¿Qué tan importante es la **seguridad de TI** para su empresa?
    [ ] Muy importante
    [ ] Importante
    [ ] Regularmente importante
    [ ] Poco importante

8. ¿Está su empresa capacitando a su personal para afrontar los problemas de **seguridad de TI**?
    [ ] Sí
    [ ] No
9. ¿Cuál es el medio por el cual su empresa capacita a los empleados en la **seguridad de TI**?
    [ ] Intranet/Extranet
    [ ] Correo Electrónico
    [ ] Cursos/Seminarios
    [ ] Documentos Físicos
    [ ] Otro, especifique cual: _____

10. ¿Conoce usted las reglas, normas y políticas de la empresa en **seguridad de TI**?

    [ ] Si

    [ ] No

11. ¿Cree usted que las reglas, normas y políticas de la empresa en **seguridad de TI** son consecuentes con su actuar personal?

    [ ] Siempre

    [ ] Casi siempre

    [ ] Nunca

12. ¿El proceso de comunicación utilizado en la empresa sobre la **seguridad de TI** considera que es?

    [ ] Bueno

    [ ] Regular

    [ ] Malo

13. ¿Cree usted que sus logros personales sobre el conocimiento de la **seguridad de TI** se están cumpliendo en la empresa?

    [ ] Siempre

    [ ] Casi siempre

    [ ] Nunca

14. ¿Se considera usted parte importante en la de **seguridad de TI** de su empresa?

    [ ] Si

    [ ] No

15. ¿Si hay un incidente de **seguridad de TI** en su empresa (Por ejemplo, robo de información, alteración de datos, acceso indebido a un sistema de computo, virus, etc.) usted lo reporta al área encargada?

    [ ] Si

    [ ] No

16. ¿Cuál es el área encargada de manejar la **seguridad de TI** de su empresa?

    [ ] Tecnología/Sistemas

    [ ] Administrativo

    [ ] Contraloría/Auditoria

    [ ] Ventas

    [ ] Mercadeo

    [ ] Producción

    [ ] Otro, especifique cual: _____

17. ¿En su empresa lo han tenido en cuenta para el desarrollo de la estrategia de la **seguridad de TI**?

    [ ] Si

    [ ] No

18. ¿Es usted consciente y conoce los riesgos y las medidas preventivas correspondientes a cumplir con la **seguridad de TI**?

    [ ] Si

    [ ] No

19. ¿Ha sido difícil el cambio de su trabajo convencional al trabajo cumpliendo los parámetros de la **seguridad de TI**?

    [ ] Si

    [ ] No

20. ¿En su empresa le hacen monitoreo y seguimiento al manejo de la información de la organización?

    [ ] Si

    [ ] No

21. ¿Considera que el tema de **seguridad de TI**, es algo muy complejo, difícil de aprender y un duro de asimilar?

    [ ] Si

    [ ] No

22. Su empresa es al día de hoy en el manejo de la información basada en las políticas de **seguridad de TI**:

    [ ] Más Segura

    [ ] Igual de Segura

    [ ] Menos Segura

23. Sus compañeros de trabajo opinan sobre **seguridad de TI** que es para la organización:

    [ ] Muy Importante

    [ ] Importante

    [ ] No influye/No afecta

    [ ] Poco Importante

    [ ] Nada Importante

    [ ] Una pérdida de tiempo

24. ¿Ha tenido usted incidentes de **seguridad de TI**?

    [ ] Si

    [ ] No

25. ¿El personal directivo de su empresa los incentiva y los apoya en el proceso de **seguridad de TI**?

    [ ] Si

    [ ] No

26. ¿Existe un verdadero compromiso de su empresa en la **seguridad de TI**?

    [ ] Si

    [ ] No

2.6.2. Tabulación y síntesis argumentativa del instrumento estadístico

Pregunta 1. ¿Cuál es el sector primario de su empresa?

Se realizó la encuesta en empresas de la cuidad de medellín, se escogió que los sectores encuestados fueran los más representativos, y que tuviesen diferentes tipos de cultura organizacional, para saber si existe una mayor cultura en unos sectores que en otros.

Se hizo mayor enfasis en las empresas en las que su principal ventaja competitiva está representada en los sistemas de información que poseen, esto nos dio certeza de cómo es el comportamiento en la seguridad de TI, en dichas empresas. Estos sectores se representaban principalmente en educación, seguros y servicios financieros/inversiones/banca, cada uno representó en su respectivo orden el 24%, 23% y 15%. Aunque tambien se consideranron otros sectores para ver el comportamiento global en el manejo de la seguridad de TI.

Tabla 11. ¿Cuál es el sector primario de su empresa?

	Cantidad	%
Servicios Financieros /Inversiones/Banca	10	15%
Construcción/Ingeniería	0	0%
Educación	16	24%
Gobierno/Sector Público/Servicios Públicos	0	0%
Seguros	15	23%
Transporte	5	8%
Tecnología / Telecomunicaciones	8	12%
Manufactura/Industria/Alimentos	7	11%
Salud	5	8%
TOTAL	**66**	**100%**

Pregunta 2. ¿Cuántos empleados tiene su organización (Incluye Temporales y Subcontratados)? ¿Si su empresa es una Multinacional, por favor indique los empleados en Colombia?

La mayor parte de las empresas encuestadas con un 59% fueron empresas que se consideran grandes, y en donde el manejo de la cultura de seguridad de TI, es más complejo debido a la cantidad de personas que interactúan entre si. Normalmente, estas empresas grandes, tienen una mayor inversión en tecnología lo que hace que deban invertir más en la seguridad de TI, y fortalecer la relación

del recurso humano con el buen manejo y el cuidado de los sistemas de información; este 59%, estuvo representado en empresas que tenían de 1000 a 2500 empleados con el 23%, y empresas con más de 2500 el 36%.

Tabla 12. ¿Cuántos empleados tiene su organización?

	Cantidad	%
Menos de 100	3	5%
De 101 a 500	13	20%
De 500 a 1000	11	17%
De 1000 a 2500	15	23%
Más de 2500	24	36%
TOTAL	**66**	**100%**

Se encontró que buen número de empleados, a pesar de llevar muchos años en las organizaciones y de interactuar diario con sus compañeros, no sabían con certeza cuántos empleados habían en sus empresas.

Aquí es interesante observar si las empresas medianas y pequeñas influyen en la cultura de seguridad de TI, ya que son empresas que no manejan mucha cultura alrededor de ello, y que debido a su tamaño, no hacen grandes inversiones en tecnología casi siempre por los bajos presupuestos que se le asignan.

Pregunta 3. ¿Cuál es su cargo en la organización?

Tabla 13. ¿Cuál es su cargo en la organización?

	Cantidad	%
Secretaria/Auxiliar	11	17%
Analista	25	38%
Jefe/Ejecutivo/Coordinador	6	9%
Director	5	8%
Gerente	2	3%
Apoyo	1	2%
Investigador	1	2%
Asistente	1	2%
Técnico Emisor	1	2%
Cajero	3	5%
Asesor	4	6%
Supernumerario	2	3%
Profesor	2	3%
Administrador de Incentivos	1	2%
Cartera	1	2%
TOTAL	**66**	**100%**

En los cargos analizados, se encontró que la mayor parte de la población encuestada no eran personal directivo, esto beneficia significativamente los resultados, toda vez que son los usuarios de los primeros niveles de la jerarquía organizacional los que realmente están interactuando día a día con los sistemas de información, y son estos empleados los que mayormente son potenciales transgresores de las políticas y en general de la seguridad de TI. Es a éste tipo de

empleados que debe ir encaminada toda la estrategia del manejo de la información para lograr en la empresa una adecuada cultura organizacional. Son el 80 % de la muestra y están principalmente constituidos por Analistas con el 38% y Auxiliares/Secretarias con el 17%. El resto del personal era de varios cargos al interior de la organización. Sólo el 20%, estuvo constituido por personal directivo, esta muestra es interesante desde el punto de vista del incentivo que le dan éstas personas a sus empleados a cargo, y observar como los motivan en el buen uso de los sistemas de información y el cómo fortalece la cultura de la seguridad de TI.

Pregunta 4. ¿Cuál es área en la que se desempeña?

Las áreas de Tecnología/Sistemas, Administrativo y Ventas, son las principales encuestadas; haciendo que se tenga una gran fiabilidad en los resultados respecto a la cultura de seguridad de TI, ya que fueron las áreas que más influencia tienen en este tema.

El área de tecnología, nos garantiza validar que los procesos de seguridad de TI existen en la compañía, y el área administrativa como él área de manejo de personal que es la encargada de educar, planear y manejar todos los procesos con miras al éxito en la empresa de una adecuada cultura organizacional. Ahora, se consideran que el resto de las áreas que encuestamos nos dan certeza de si está activa, vigente y en la cultura de la organización la seguridad de TI.

Tabla 14. ¿Cuál es área en la que se desempeña?

	Cantidad	%
Tecnología/Sistemas	20	30%
Administrativo	16	24%
Contraloría/Auditoria	0	0%
Ventas	12	18%
Mercadeo	1	2%
Producción	3	5%
Logística de Exportaciones	1	2%
Investigación	3	5%
Comunicaciones	1	2%
Servicios	2	3%
Comercial	1	2%
Operativo	1	2%
Cajero	2	3%
Asesoría en Riesgos y Seguros	1	2%
Docencia	2	3%
TOTAL	**66**	**100%**

Pregunta 5. ¿Qué tan frecuentemente usa Internet para su trabajo?

Tabla 15. ¿Qué tan frecuentemente usa Internet para su trabajo?

	Cantidad	**%**
Constantemente	52	79%
Ocasionalmente	10	15%
Raramente	1	2%
Nunca	3	5%
TOTAL	**66**	**100%**

Se encuentra algo muy interesante con esta pregunta, y es que cada día las empresas y específicamente sus empleados están mas ligados a Internet, y dependen de él como fuente para complementar los sistemas de información de la organización, se observa que el 79% de los empleados están costantemente utilizando Internet como herramienta de trabajo. Este parámetro es muy importante debido a los problemas que daños, perdida o alteración de la información involuntaria de los empleados al ingresar a sitios que pueden por medio de virus, madware, spyware, etc. que son los que ejecutan los problemas en los sistemas de información de la empresa. También porque Internet es un medio que permite facilmente el robo de información en las empresas por medio de los sitemas de almacenamiento de información en la WEB, y por los correos gratuitos, éste último adicionalmente es utilizado por muchas empresas para abrir cuentas de correo y utilizarlas como correos corporativos.

Pregunta 6. ¿Tiene la empresa en la cual trabaja una estrategia de Seguridad de TI?

Tabla 16. ¿Tiene la empresa en la cual trabaja una estrategia de seguridad de TI?

	Cantidad	**%**
Sí	62	94%
No	3	5%
NS / NR	1	2%
TOTAL	**66**	**100%**

Se encontró que el 94% de las empresas encuestadas tienen implementada una estrategia de seguridad de TI, este valor es importante debido que se preocupan por proteger sus recursos informáticos y especialmente los sistemas de información. En general, se evidencia que las empresas están destinando recursos tanto humanos como informaticos para el control y la gestión de la información, lo que les permite fortalecerse como compañias integrales que se preocupan por sus clientes y por su información. Nos permite inferir esta pregunta que la mayoria de las empresas han divulgado sus procesos de seguridad de TI, ya que los empleados conocen que existe una estrategia de seguridad de TI.

Pregunta 7. ¿Qué tan importante es la Seguridad de TI para su empresa?

Tabla 17. ¿Qué tan importante es la seguridad de TI para su empresa?

	Cantidad	**%**
Muy importante	49	74%
Importante	12	18%
Regularmente importante	4	6%
Poco importante	0	0%
NS / NR	1	2%
TOTAL	**66**	**100%**

Es impórtante conocer que el 74 % de los empleados consideran que los sistemas de información son un componente muy importante en la organización, pero tambien que el 18% saben que es muy importante, esto influye en los empleados lo que los hace más concientes de proteger la información por medio de los procedimientos implementados de seguridad de TI.

A considerar los empleados que la seguridad de TI es importante en la empresa los hace reflexionar sobre la forma como ellos manejan la información y sobre como la deben manejar con el fin de no transgredir los principios de la seguridad de TI.

El 8 % restante, hace pensar en las empresas que les está fallando o que no tienen procesos de seguridad implementados, este 8% es congruente con el 7 % de la empresas que no tienen implementado sistemas de seguridad de TI.

Pregunta 8. ¿Está su empresa capacitando a su personal para afrontar los problemas de seguridad de TI?

Tabla 18. ¿Está su empresa capacitando a su personal para afrontar los problemas de seguridad de TI?

	Cantidad	%
Sí	49	74%
No	16	24%
NS / NR	1	2%
TOTAL	**66**	**100%**

Tenemos cifras que deben ser precupantes en las empresas ya que al tener el 24 % de los empleados sin capacitación sobre seguridad de TI, hace que la empresa este obligada a desarrollarar una estrategía de seguridad de TI, así, si su seguridad falla tarde o temprano, por lo que hemos mensionado anteriormente, tiene que tener una estrategia de protección en seguridad. Pasa aquí que los usuarios son suceptibes a alterar la información por desconocimiento, por robo, etc.

Pero al tener el 74 % de las empresas enfocadas en divulgar todo su trabajo, y toda su labor de seguridad de TI en la organización, hace que estás empresas esten influyendo en la cultura de la empresa haciendo que la seguridad de TI se convierta en una variable en la organización.

Pregunta 9. ¿Cuál es el medio por el cual su empresa capacita a los empleados en la seguridad de TI?

Tabla 19. ¿Cuál es el medio por el cual su empresa capacita a los empleados en la seguridad de TI?

	Cantidad	%
Intranet/Extranet	35	38%
Correo Electrónico	16	18%
Cursos/Seminarios	23	25%
Documentos Físicos	7	8%
Personal	1	1%
Ninguno	3	3%
NS / NC	6	7%
TOTAL	**91**	**100%**

Es algo, cuestionable que el 75 % de las empresas tengan estrategías de autoaprendizaje, esto es por que no permite a los empleados tener medios eficientes para resolver sus dudas, y principalmente por que la educación a distancia requiere un compromiso muy alto del empleado.

El 25 % de las empresas hacen una educación personalizada, esto es mucho más efectivo que la educación a distancia por que los empleados pueden interactuar con los profesores, resolver dudas, y conocer más detalladamente en que consiste y cuales son los procesos de seguridad de TI en la empresa. Aquí, los medios escritos, que se utilizan para educación a distancia (el otro 25 %) es un complemento muy importante ya que permite a los empleados realizar consultas

sobre los cursos dictados, o para hacer actualizaciónes de conocimiento en el tema.

Pregunta 10. ¿Conoce usted las reglas, normas y políticas de la empresa en seguridad de TI?

Tabla 20. ¿Conoce usted las reglas, normas y políticas de la empresa en seguridad de TI?

	Cantidad	**%**
Si	47	71%
No	18	27%
NS / NR	1	2%
TOTAL	**66**	**100%**

El 71 % de los empleados, se han precoupado por conocer las politicas de la empresa en seguridad de TI, esto hace que el conocimiento del tema sea exitoso, y que se pueda inculcar en la empresa una cultura de seguridad de TI.

El 29% restante son empresas que están fallando en su proceso de capacitación en seguridad de TI, que tienen que asignar recursos, tiempo y empeñarse a fortalecer en los empleados el buen uso de los sistemas de información.

Pregunta 11. ¿Cree usted que las reglas, normas y políticas de la empresa en seguridad de TI son consecuentes con su actuar personal?

Tabla 21. ¿Cree usted que las reglas, normas y políticas de la empresa en seguridad de TI son consecuentes con su actuar personal?

	Cantidad	%
Siempre	38	58%
Casi siempre	21	32%
Nunca	3	5%
NS / NC	4	6%
TOTAL	**66**	**100%**

Solo encontramos que el 58 % de los empleados, realmente están permanentemente concientes y preocupados por la información de la empresa y por empeñarse en cumplir con la seguridad de TI implementada.

Es cuestionable que el 32 % de los empleados de las compañías, sepan que la información es un valioso activo de la empresa, pero que a pesar de conocer y aplicar la seguridad de TI, también hacen cosas que ponen en peligro la información por no ser consecuentes con su actuar en algunas ocasiones y hacer cosas que permitiran que la seguridad falle.

Pregunta 12. ¿El proceso de comunicación utilizado en la empresa sobre la seguridad de TI considera que es?

Tabla 22. ¿El proceso de comunicación utilizado en la empresa sobre la seguridad de TI considera que es?

	Cantidad	%
Bueno	47	71%
Regular	13	20%
Malo	5	8%
NS / NC	1	2%
TOTAL	**66**	**100%**

Todos los medios de comunicación que han implementado en las compañías para enseñar los procesos de seguridad de TI, han hecho que sólo el 71% de los empleados lo vean como exitoso, esto puede ser debido a la gran cantidad de medios escritos que emplean y lo poco que hacen capacitaciones por medio de cursos o seminarios, de ahí que se refleje que el 29% consideren regular o mala la forma de comunicar un proceso tan importante para la compañía como es la seguridad de TI.

Pregunta 13. ¿Cree usted que sus logros personales sobre el conocimiento de la seguridad de TI se están cumpliendo en la empresa?

Pregunta que nos corrobora el éxito de la seguridad de TI, sólo tenemos que el 41% están sintiendo que su actuar se articula con las politicas definidas, y se

preocupan por mantener la información a salvo. Se nota una debilidad en la cultura de seguridad de TI en las organizaciones al conocer que el 59 % de los empleados, cumplen parcialmente o no cumplen a cabalidad con el compromiso que tienen con el buen uso de los sistemas de información debido a no interiorizar y aplicar constantemente las politicas definidas por la compañía.

Tabla 23. ¿Cree usted que sus logros personales sobre el conocimiento de la seguridad de TI se están cumpliendo en la empresa?

	Cantidad	**%**
Siempre	27	41%
Casi siempre	30	45%
Nunca	7	11%
NS / NC	2	3%
TOTAL	**66**	**100%**

Pregunta 14. ¿Se considera usted parte importante en la de seguridad de TI de su empresa?

Tabla 24. ¿Se considera usted parte importante en la de seguridad de TI de su empresa?

	Cantidad	**%**
Si	53	80%
No	10	15%
NS / NC	3	5%
TOTAL	**66**	**100%**

Que importante es para las organizaciones saber que los empleados conocen que los procesos de seguridad de TI, y se pudo corroborar en el 80 % de empleados que se consideran fundamentales y que son participantes activos en la protección de los sistemas de información. De igual manera, esta pregunta es consecuente con anteriores en donde se observa que el 74% saben que es Muy importante la seguridad de TI y que el 71 % conoce las reglas y políticas de seguridad de TI.

Nuevamente, ¿Qué está pasando con el 20% restante?, puede exitir una cifra tan alta debido a las fallas en comunicación o a la debil estrategia de capacitación personal en las empresas, lo que también es congruente con las preguntas anteriores.

Pregunta 15. ¿Si hay un incidente de seguridad de TI en su empresa usted lo reporta al área encargada?

Tabla 25. ¿Si hay un incidente de seguridad de TI en su empresa usted lo reporta al área encargada?

	Cantidad	**%**
Si	64	97%
No	1	2%
NS / NC	1	2%
TOTAL	**66**	**100%**

Se evidencia que el 97 % de los empleados esten en disposición de informar los problemas de seguridad que tengan o que se presenten, estó hace que el área

encargada de la seguridad de TI, esté en constante mejora y actualización de los procesos y politicas implementadas en la empresa.

Pregunta 16. ¿Cuál es el área encargada de manejar la seguridad de TI de su empresa?

Tabla 26. ¿Cuál es el área encargada de manejar la seguridad de TI de su empresa?

	Cantidad	%
Tecnología/Sistemas	56	82%
Administrativo	1	1%
Contraloría/Auditoria	7	10%
Ventas	0	0%
Mercadeo	0	0%
Producción	0	0%
Una empresa Externa	1	1%
Seguridad Bancaria	1	1%
Sistema de seguridad informática (SSI)	1	1%
NS / NC	1	1%
TOTAL	68	100%

Debemos analizar algo importante en esta pregunta, el 82% de los encuestados afirma que el área de Tecnología/Sistemas es la encargada de la seguridad de TI, luego le sigue Contraloría. Esto es lo tipico en las empresas, pero lo mínimo es

que fueran las dos áreas las encargadas al unisono de la seguridad de TI; aunque realmente lo ideal es que sea un área totalmente aparte la encargada de manejar la seguridad de TI, ésta unificaría los conocimientos de todas las demás de la organización para lograr implementar una muy robusta seguridad de TI; este caso ideal de estructura para el menejo de la seguridad tiene empleados de todas las áreas de la compañía trabajando para ellos, dedicados tiempo completo, y siempre indagando cómo mejorar la seguridad de TI en cada una de sus áreas.

Se encontró que realmente la seguridad de TI, la maneja principalmente el área de Tecnologia/Sistemas de forma autónoma, y son ellos los únicos que definen qué información es importante, qué politicas implementar, etc. Esto es una falla en el proceso.

Pregunta 17. ¿En su empresa lo han tenido en cuenta para el desarrollo de la estrategia de la seguridad de TI?

Tabla 27. ¿En su empresa lo han tenido en cuenta para el desarrollo de la estrategia de la seguridad de TI?

	Cantidad	**%**
Si	15	23%
No	49	74%
NS / NC	2	3%
TOTAL	**66**	**100%**

Si analizamos esta pregunta, es consecuente con la pregunta anterior, en donde se tiene que la mayor parte de las organizaciones (74%), implementan una

seguridad de TI, haciendo politicas, definiendo los niveles de seguridad en la información, valorando ellos mismos la información y sin tener en cuenta los usuarios, es aquí cuando las áreas encargadas, principalmente Tecnología/Sistemas, falla al no involucar a los que tienen realmente el conocimiento de la información y como se interactua con ella. Es un aspecto que las empresas en general deben mejorar.

Pregunta 18. ¿Es usted consciente y conoce los riesgos y las medidas preventivas correspondientes a cumplir con la seguridad de TI?

Tabla 28. ¿Es usted consciente y conoce los riesgos y las medidas preventivas correspondientes a cumplir con la seguridad de TI?

	Cantidad	**%**
Si	52	79%
No	13	20%
NS / NC	1	2%
TOTAL	**66**	**100%**

Tenemos una contrapregunta para valorar la fiabilidad de los datos y la congruencia en estos, observando que el 79% de los empleados, si conocen sobre seguridad de TI en su empresa, y cuáles politicas y procesos tienen implemantadas, esto nos ratifica las preguntas enteriores sobre capacitación, conocimiento de politicas y conocimiento sobre si la empresa tiene definida la seguridad de TI.

Pero al igual que se ha dicho anteriormente el 20% de las empresas deben mejorar para lograr un mayor porcentaje de cubrimiento sobre seguridad de TI por parte de los empleados.

Pregunta 19. ¿Ha sido difícil el cambio de su trabajo convencional al trabajo cumpliendo los parámetros de la seguridad de TI?

Tabla 29. ¿Ha sido difícil el cambio de su trabajo convencional al trabajo cumpliendo los parámetros de la seguridad de TI?

	Cantidad	**%**
Si	13	20%
No	50	76%
NS / NC	3	5%
TOTAL	**66**	**100%**

Muy importante es que la mayoria de los empleados, asimilen de forma natural y no de forma forzosa o compleja la seguridad de TI en las empresas, esto facilita el proceso, fortalece la cultura de seguridad de TI, y garantiza que sea exitosa. También nos dice que los empleados, tienen un alto compromiso ya que hicieron esfuerzos para implementar rápidamente la seguridad de TI en su diario laborar.

Pregunta 20. ¿En su empresa le hacen monitoreo y seguimiento al manejo de la información de la organización?

Tabla 30. ¿En su empresa le hacen monitoreo y seguimiento al manejo de la información de la organización?

	Cantidad	%
Si	55	83%
No	11	17%
TOTAL	**66**	**100%**

Esta pregunta ratifica que los empleados son consientes que son responsables de los sistemas de información, y que la empresa está permanentemente revisando que los empleados si cumplan con las normas y políticas definidas con respecto a la información.

Pregunta 21. ¿Considera que el tema de Seguridad de TI, es algo muy complejo, difícil de aprender y un duro de asimilar?

Tabla 31. ¿Considera que el tema de seguridad de TI, es algo muy complejo, difícil de aprender y un duro de asimilar?

	Cantidad	%
Si	5	8%
No	59	89%
NS / NC	2	3%
TOTAL	**66**	**100%**

Lo fácil de aprender y ofrecer menos resistencia al cambio, la mayoria de los empleados (89%) precisa que la seguridad de TI no es un tema dificil, complejo y que altera su diario trabajar, hace que la cultura de seguridad de TI se fortalezca. Así, los empleados apoyaran los procesos, y ayudaran la empresa cada día a mejorar los sistemas de información en todos los aspectos tecnologícos y de seguridad.

Pregunta 22. Su empresa es al día de hoy en el manejo de la información basada en las políticas de seguridad de TI:

Tabla 32. Su empresa es al día de hoy en el manejo de la información basada en las políticas de seguridad de TI

	Cantidad	**%**
Más Segura	48	73%
Igual de Segura	17	26%
Menos Segura	0	0%
NS / NC	1	2%
TOTAL	**66**	**100%**

Las empresas hacen que los empleados se sientan mas seguros con los procesos de seguridad de TI implementados, esto nuevamente nos dice que la cultura de seguridad de TI es exitosa, y que le da tranquilidad a la organización, que a su vez es transmitida a los clientes.

Pregunta 23. Sus compañeros de trabajo opinan sobre seguridad de TI que es para la organización:

Tabla 33. Sus compañeros de trabajo opinan sobre seguridad de TI que es para la organización

	Cantidad	%
Muy Importante	27	41%
Importante	26	39%
No influye/No afecta	8	12%
Poco Importante	3	5%
Nada Importante	0	0%
Una pérdida de tiempo	0	0%
NS / NC	2	3%
TOTAL	**66**	**100%**

Otra pregunta que sirve para validar la cultura de seguridad informática, entre los empleados, es normal que se comparta información y se trasmitan sus percepciones sobre los temas de la organización, uno de ellos es la seguridad de TI, al observar que el 41 % y 39 % consideran Muy importante e Importante respectivamente, que entre los compañeros la seguridad de TI es algo estratégico para la empresa, hace que todos los empleados esten sintonizados con la estrategia y se fortalezca la cultura de seguridad de TI.

Pregunta 24. ¿Ha tenido usted incidentes de seguridad de TI?

Tabla 34. ¿Ha tenido usted incidentes de seguridad de TI?

	Cantidad	%
Si	10	15%
No	55	83%
NS / NC	1	2%
TOTAL	**66**	**100%**

Como los empleados sienten que las empresas son más seguras, tenemos una pregunta que nos confirma con el hecho de tener una baja cantidad de incidentes de seguridad de TI, al igual que se expresó anteriormente esto ofrece tranquilidad a los empleados en los sistemas de información y facilita un mayor arraigo de las politicas y procesos de seguridad de TI.

Pegunta 25. ¿El personal directivo de su empresa los incentiva y los apoya en el proceso de seguridad de TI?

Tabla 35. ¿El personal directivo de su empresa los incentiva y los apoya en el proceso de seguridad de TI?

	Cantidad	%
Si	47	71%
No	18	27%
NS / NC	1	2%
TOTAL	**66**	**100%**

Es muy importante que los directivos de las organizaciones apoyen el proceso de seguridad de TI, y propendan a fortalecerlo, ya que son ellos, los que realmente influyen directamente sobre la cultura de la organización; entonces si esto se logra tendremos que se tendra una cultura de seguridad de TI en las empresas y organizaciones.

Pregunta 26. ¿Existe un verdadero compromiso de su empresa en la seguridad de TI?

Tabla 36. ¿Existe un verdadero compromiso de su empresa en la seguridad de TI?

	Cantidad	**%**
Si	51	77%
No	12	18%
Algunas Veces	1	2%
NS / NC	2	3%
TOTAL	**66**	**100%**

Nos corrobora todas las respuestas encontradas en la investigación, y es que las empresas encuentran valiosa la información y buscan proteger los sistemas de información, por medio de la seguridad de TI. Y al interiorizar la seguridad de TI en los empleados logran que ésta haga parte constitutiva de la cultura de la misma.

En conclusión, encontramos que si existe una variable en la cultura de la organización que se llama seguridad de TI, que lo podríamos denominar de otra manera, es decir, cultura de seguridad de TI. Esto se confirma con los valores que arrojados por la encuesta, y en los que se infiere claramente la importancia de la información para las empresas, asimismo, en el compromiso de los empleados y de la empresa como tal, con los procesos de capacitación y en los aspectos que ya observamos en la encuesta, con lo cual se puede aseverar el valor de los sistemas de información y la proteción de los mismos como referente constitutivo de la cultura organizacional.

Con base en la prueba empírica anterior, se proponen como sustrato teórico que puede ser aplicado en la práctica el siguiente modelo:

2.6.3. Etapas para desarrollar un modelo de seguridad de TI

1. **Definición del mundo:**
   En esta etapa se pretende entender claramente el mundo al cual se le quiere hacer el estudio de seguridad.

2. **Análisis de riesgos e impactos**
   El propósito del análisis de riesgos e impactos es determinar cuáles son las amenazas reales que existen para la empresa y de qué manera éstas pueden ser mitigadas, ya sea evitando su ocurrencia y/o disminuyendo su impacto. Los siguientes términos son básicos en el análisis de riesgos e impactos:
   - **Bien**: Algo con valor para la institución que necesita ser protegido.

- **Amenaza:** Una acción o acción potencial con posibilidad de causar daño.
- **Vulnerabilidad:** Condición de debilidad. Al no existir vulnerabilidades, las amenazas no tendrían impacto alguno en la institución.
- **Impacto:** Aquellas pérdidas producto de la actividad de las amenazas. Estas pueden manifestarse como destrucción, interrupción, modificación y exposición de los bienes de la institución.
- **Riesgo:** la probabilidad de que un evento adverso ocurra contra un bien.
- **Riesgo residual:** Riesgo que permanece después de aplicar medidas de mitigación a un riesgo.

3. Diseño de las políticas de seguridad

Las políticas deben ser determinantes para la evaluación y/o selección de los mecanismos de seguridad. Algunas políticas podrían, por ejemplo, restringir el adquirir cierto tipo de mecanismos. Cuando se diseñan políticas se debe tener en cuenta los siguientes aspectos:

- **Conocimiento del entorno:** Las leyes que rigen el negocio, tipo de negocio, competencia, características tecnológicas y negocios estratégicos de la institución.
- **Material de referencia:** Diccionario de base de datos, arquitectura de la red, futuro tecnológico basado en estándares;
- **Conocimiento de la cultura interna:** Revisa las normas de otras áreas, adquisición de equipos, capacitación, recursos humanos, aseguramiento de calidad, seguridad física,
- **Determinación de servicios informáticos críticos:** Establece los servicios catalogados como críticos de la institución,
- **Matriz de cubrimiento:** Después de tener el área de cubrimiento se debe clasificar en forma macro en donde se tengan identificados los servicios informáticos y las diferentes categorías determinadas. En el

cruce de la categoría de la política con el servicio, se establece el tipo de control y su objetivo (prevenir, detectar, recuperar, corregir, evitar). Como resultado de cada uno de los objetivos buscados por las categorías determinadas, se debe establecer la herramienta a utilizar y/o el procedimiento para alcanzar el objetivo.

- **Presentación al comité de aprobación:** la matriz es muy clara y es una herramienta para obtener la aprobación de las políticas asociadas.
- **Divulgación:** Proceso para garantizar el debido conocimiento por parte de las personas de la institución
- **Evaluación:** Es necesario evaluar y actualizar las políticas existentes de acuerdo a la evolución del negocio y a los cambios tecnológicos.

4. Diseño de los mecanismos de seguridad

Los mecanismos de seguridad que deben ser diseñados o tenidos en cuenta (los que ya existen en la Institución), son el resultado de los múltiples análisis de riesgos y de las políticas de seguridad que hayan sido definidas.

CONCLUSIONES

- Ninguna institución, sin importar su tamaño, puede desconocer la naturaleza e importancia de la seguridad informática, debido al auge de las comunicaciones que permiten integrar cada día más las aplicaciones. Aplicar la seguridad sin seguir metodologías puede en ocasiones ser aún más riesgoso que no aplicarla. De la misma manera, no existe metodología alguna que cubra un 100% la totalidad de los aspectos de seguridad, debido al gran cubrimiento que tiene la seguridad.

- Como resultado puntual, la investigación nos permite ratificar que la seguridad de TI es no sólo una variable de la cultura organizacional sino también que es el referente en el cual se leen en la actualidad la mayor parte de las empresas y organizaciones, gracias al cambio de mentalidad operado por el uso de las tecnologías informacionales y por vivir las dinámicas y exigencias de un mundo globalizado en el cual, todo gira alrededor de la información y de las tecnologías que la soportan. Por lo tanto, la cultura organizacional es y será el continuum de los cambios operados en los contextos donde interactúan y de los cambios que debe incorporar hacia dentro en tecnología, procesos, políticas, estrategias, metodologías, estándares, actitudes, ideas y aptitudes cada una de las organizaciones.

  .

BIBLIOGRAFIA

ABARBANEL, H. Cultura organizacional, Aspectos Teóricos, prácticos y metodológicos. Bogotá: Ed. Legis, 2005. 489p

ABRAHAMS, Jeffrey. The Mission Stament Book: 301 Corporate Staments from America´s Top Companies. USA: Ten Speed Press. 1996. 512 p. ISBN-10: 1580081320

ÁBRALE; ALLAIRE y OTROS. Cultura organizacional. Aspectos teóricos prácticos y metodológicos. Bogotá. LEGIS, 1992. p.16-18.

ALMANZA J., Andrés Ricardo. Responsable de la inseguridad de la información. En: SISTEMAS, Santa Fe de Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 105. Abril-Junio 2008. p.63-64

AROCENA, José. Cambio organizacional. En:Prisma. Montevideo: Universidad Católica de Uruguay. No. 10. 1998. p.42-51

AUSTIN, Robert D.; DARBY, Christopher A.R. El mito de la Seguridad Informática. En: Harvard Deusto Business Review. Barcelona. No. 120. Enero 2004. p. 66-74

BARRERA R., Efrén. Cinco hitos que modifican la cultura empresarial. En: Revista Antioqueña de economía y desarrollo. Medellín. No.57. 1999. p.96-99

BARRIENTOS ARCILA, Andrea Marcela; AREIZA CÓRDOBA, Alexandra. Integración de un Sistema de gestión de seguridad de la información con un Sistema de Gestión de la Calidad. Medellín: Universidad Eafit. 2005.

BIDOT PELÁEZ, José. Seguridad informática en Latinoamérica. En: Innovación, Ciencia y Desarrollo. Cuba. Vol 2 No. 1. 1996. p. 28-31

BLANCHARD, Ken; CARLOS, Jhon P; RANDOLPH, Alan. Empowerment: 3 claves para lograr que el proceso de facultar a los empleados funcione en su empresa. Bogotá: Norma, 2002. 94p.

BLANCHARD, Ken;O'CONNOR, Michael. Administración por valores: Cómo lograr el éxito organizacional y personal mediante el compromiso con una misión y unos valores comparativos. Bogotá: Norma, 1997. 150p.

CALDAS LEMAITRE, Rodrigo. Seguridad informática ¿Una política empresarial? En: SISTEMAS, Santa Fe de Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 89. Julio-Septiembre 2004. p.1-2

CANO, Jeimy J. Administrando la confidencialidad de la información. En: SISTEMAS, Santa Fe de Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 101. Julio-Septiembre 2007. p. 62-69

CANO, Jeimy J. Inminente toma de conciencia. En: SISTEMAS, Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 85. Junio-Julio 2003. p. 2-4

CANO, Jeimy J. Inseguridad informática: Un concepto dual en seguridad informática. En: Revista de Ingeniería, Bogotá: Universidad de los Andes. No. 19. 2004. p. 40-44

CANO, Jeimy J. La seguridad informática y los procesos de negocio: ¿dos mundos distintos?. En: SISTEMAS. Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 104. Enero-Marzo 2008. p. 53-61

CANO, Jeimy J. Monitoreo y evolución de la seguridad de la información. En: SISTEMAS, Bogotá: Asociación Colombiana de Ingenieros de Sistemas-ACIS-. No. 110. Abril-Junio 2009. p.4-13

CARVER, John. CarverGuide, Creating a Mission That Makes a Difference. New York: Jossey-Bass. 1996. 24 p. ISBN-10: 0787903027

CONTRERAS, Francoise. Leadership: Prospects for Development and Research. In: International Journal of Psychological Research. 2008. p. 42. ISSN 2011 - 7922.

DALTABUIT, Enrique; HERNÁNDEZ, Leobardo; MALLEN, Guillermo; VÁSQUEZ, José. La seguridad de la información. México: Ed. Limusa. 2007. p.233-263.

DAY, K. Inside the security mind. Making the tough decisions. Prentice Hall. 2003. p.5.

DENISON, Daniel R. Cultura Corporativa y productividad organizacional. Bogotá: Legis, 1991. 238p.

ECHAVARRÍA J., María Teresa. Componentes de la cultura organizacional. En: Pensamiento & Gestión, Barranquilla: Universidad del Norte. No. 9. 2000. p.42-55.

ETKIN, Jorge. La Doble Moral de las organizaciones. Sistemas Perversos y Corrupción Institucionalizada. México: Mc. Graw Hill Editores. 1994.

ETKIN, Jorge. La empresa competitiva: Grandeza y decadencia el cambio hacia una organización vivible. Santiago de Chile: Mc.Graw Hill, 1996. 356p

FERRIS, J. M. Using Standards As A Security Policy Tool. In: StandartView. New York: ACM Press. Volume 2, Issue 2. June, 1994. p. 72-77. ISSN:1067-9936.

FOSTER, George M. Antropología Aplicada. México: Fondo de cultura Económica. 1974. p.54

GARCÍA VARGAS, Oscar Humberto. La cultura humana y su interpretación desde la perspectiva de la cultura organizacional. En: Pensamiento & Gestión, Barranquilla: Universidad del Norte. No. 22. 2007. p. 151

GEERTZ, Clifford. La interpretación de las culturas. Buenos Aires: Gedisa. 1990. 289p

GUIOT, Jean M., BEAUFILS, Alain. Diseño de la organización: Del cargo a la mega estructura. Bogotá: Legis, 1992. 227p.

GUZMAN N., Arcadio José. Entorno organizacional. Cali: Universidad del Valle. Facultad de ciencias de la administración, 1998. 244p.

HUERTAS A., Juan Carlos. Seguridad Corporativa. En: SISTEMAS, Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS. No. 77. Enero-Junio 2000. p. 50-61

JAUCH, Lawrence R.; GLUECK, William F. Business Policy and Strategic Management. USA: McGraw-Hill Companies. 1988. 960 p. ISBN-10: 0071005072.

KROEBER, A.; KLUCKHOHN, C. Culture. A Critical Review of Concepts and definitions. In: Papers of the Peabody Museum, Cambridge, Harvard University Press. Vol. XLVII: 1. 1952. p.37

LALINDE PULIDO, Juan Guillermo y Otros. Hacia un Modelo de Madurez para la seguridad de la información. Medellín: Universidad Eafit. 2005.

LEVI-STRAUSS, Claude. Antropología estructural: Mito, sociedad, humanidades. Barcelona: Editorial Paidós Ibérica. 1986. p.142

LINTON, Ralph. Cultura y personalidad. México. Fondo de cultura Económica. 2005.p.124

LÓPEZ, Jaquelina. Los Criterios comunes sobre evaluación de la confiabilidad de tecnologías de la información. México: Universidad Nacional Autónoma de México. 2001.

MALINOWSKI, Bronislaw. Los argonautas del Pacífico Occidental. Barcelona: Península. 1985. p.50

MÉNDEZ ÁLVAREZ, Carlos Eduardo. Metodología para describir la cultura organizacional: estudio de caso en una empresa colombiana del sector industrial.

En: Universidad y Empresa, Santafé de Bogotá: Universidad del Rosario. No. 7. 2004. p.51-81

MÉNDEZ ÁLVAREZ, Carlos Eduardo. Transformación cultural en las organizaciones: Un Modelo para la Gestión del Cambio. Bogotá: Ed. Limusa. 2009. p.78

MORGAN, Gareth. Imágenes de la organización. México: Alfaomega, 1995. 408p.

NHOLAN, Richard. Destrucción Creativa. México: Mc. Graw Hill Editores. 1996.

PELTIER, Thomas R. Information Security Risk Analysis. USA: Auerbach. 2005. 296 p. ISBN-10: 0849308801.

PEÑA, Dary Sandra. Seguridad: Una cultura en formación. En: COMPUTERWORLD. Vol. 14, No. 203 (Abr.-May., 2003); p. 10-11.

PÉREZ GARCÍA, Antonio. De identidades y de organizaciones. En: Prisma, Montevideo: Universidad Católica de Uruguay. No. 10. 1998. p.7-41

RIBAGORDA GARNACHO, Arturo. Tecnologías de la información. En: Innovación, Ciencia y Desarrollo, Cuba. Vol 2 No. 1. 1996. p. 39-44

RIVAS D., Luis Francisco. Cultura organizacional. En: Memos de Investigación, Santafé de Bogotá: Universidad de los Andes. No. 107, 1993. p2

RIVAS D., Luis Francisco. Seguridad informática en las organizaciones. En: SISTEMAS, Bogotá: Asociación Colombiana de Ingenieros de Sistemas ACIS . No. 76. p. 64-71

RIVERA, Carmen Cecilia. Descripción de cultura organizacional. En:Dia-Logos , Perú: Revista de la federación latinoamericana de facultades de comunicación social FELAFACS . No. 39. 1994. p. 36-41

RODRÍGUEZ D., Eduardo. Los laberintos del cambio organizacional. En: Revista Colombiana de Psicología, Santafé de Bogotá: Universidad Nacional de Colombia. No. 3. 1994. p.66-72

SCHNEIER, B. Security and compliance. En: IEEE Security & Privacy, USA. July/August. 2004. p.3.

SORONDO, Fernando. Cultura, Cambio y Aprendizaje en las organizaciones. En:Prisma, Montevideo: Universidad Católica de Uruguay. No. 10. 1998. p. 42-51

SUMMERS, Rita C. Secure Computing: Threats and Safeguards. USA:Mc.Graw Hill.1996. p.1-11

TAMAYO A., Alonso; DUQUE M., Néstor D. ¿Cómo se deben controlar los sistemas de información?. En: NOOS, Manizales: Universidad Nacional de Colombia. No. 18. 2004. p. 129-130.

TAMAYO A., Johnny., TAMAYO A., Alonso. Auditoría y seguridad informática. En: NOOS, Manizales: Universidad Nacional de Colombia. No. 18. 2004. p. 78-88

TANEY Jr., F.; COSTELLO, T. Securing the whole enterprise: Business and legal issues. En: IEEE IT Professional, USA. January/February. 2006. p. 8-9.

TAYLOR, Charles. Una Antropología de la Identidad. Buenos Aires: Ed. Eunsa. 2002. 342p.

TAYLOR, Edward B. "La ciencia de la cultura". En: KAHN, J. S. (comp.): El concepto de cultura, Barcelona: Anagrama. 1995. p. 24

TORO ÁLVAREZ, Fernando. Distinciones y relaciones entre clima, motivación, satisfacción y cultura organizacional. En: Revista Interamericana de Psicología Ocupacional, Medellín. Vol. 17 No. 2. 1998. p. 27-40

VÁSQUEZ, María de Lourdes. A Todo Riesgo. En: IT MANAGER. Vol. 3, No. 43. May-Jun 2003. p.22-33.

WARD H. Goodenough. Description & Comparison in cultural Anthropology. Aldine Transaction, 2006. p.12

WESTNEY, E. (2008) Three perspectives on organizational change. Leading Change in Complex Organization. MIT Sloan School of Management. Executive Program. June.

@BERINATO, Scott. The Global State of Information Security 2005. Pricewaterhouse Coopers and CIO <http://www.cio.com/archive/091505/global.html> [citado en septiembre 15 de 2005]

@CHECK POINT SOFTWARE TECHNOLOGIES LTD. Check Point VPN-1/FireWall-1 Achieves Internationally Recognized ITSEC Security Certification. <http://www.checkpoint.com/0301/itsec/>. [citado en septiembre 26 de 2009]

@CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html> [citado en junio 09 de 2009]

@CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 599 de 2000. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html> [citado en junio 09 de 2009]

@CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 603 de 2000. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0603_2000.html> [citado en junio 09 de 2009]

@CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley estatutaria 1266 de 2008. <http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html> [citado en junio 09 de 2009]

@GUEL, Michele D. A Short Primer for Developing Security Policies. En: SANS Institute. 2007. 43 p. <http://www.sans.org/security-resources/policies/Policy_Primer.pdf>. [citado en Mayo 1 de 2009]

@IBM CORPORATION. Detener los ataques internos: cómo pueden proteger las organizaciones su información confidencial. <http://www-05.ibm.com/services/es/cio/pdf/CIO_Series_0302.pdf> [citado en septiembre 1 de 2006]

@INFORMATIOM SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). Control Objetives for informatiom and related technology, 2006. <http://www.isaca.org/cobit>. [citado en Septiembre 10 de 2009].

@MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO. Decreto número 1747 de 2000. <http://www.mincomercio.gov.co/eContent/documentos/normatividad/decretos/decreto_1747_2000.pdf> [citado en junio 09 de 2009]

@MINISTERIO DE COMUNICACIONES - REPUBLICA DE COLOMBIA . Decreto número 1524 de 2002. <http://www.cntv.org.co/cntv_bop/basedoc/decreto/2002/decreto_1524_2002.html > [citado en junio 09 de 2009]

@OBSERVATORIO COLOMBIANO DE CIENCIA Y TECNOLOGÍA (OCYT). Ley 527 de 1999. <http://www.ocyt.org.co/leg/Ley%20527.pdf> [citado en junio 09 de 2009]

@OFFICE FOR OFFICIAL PUBLICATIONS OF THE EUROPEAN COMMUNITIES. Information Technology Security Evaluation Criteria (ITSEC): Provisional Harmonised Criteria. <http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf>. 1991. ISBN 92-826-3004-8 [citado en Septiembre 1 de 2009]

@POLYCASTRO, Michael. Introduction to strategic planning: Management and planning series. En: U.S. Small Bussines Administration. 2004. 17 p. <http://www.sba.gov/idc/groups/public/documents/sba.../pub_mp21.pdf> [citado en 20 de abril de 2009]

@SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular externa 052 de 2007.

<http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf> [citado en junio 09 de 2009]

@THE ALLIANCE FOR ENTERPRISE SECURITY RISK MANAGEMENT (AESRMT). Security convergence and ERM. The Convergence of IT Security and Enterprise Risk Management: A Security Professional's Point of View. <http://www.aesrm.org/files/Convergence_SecProf_View_5Mar09_Research.pdf> [citado en mayo 30 de 2009]. p.5

ANEXO 1

PRECAUCIONES EN INTERNET

Muchos sitios en Internet exigen que antes de ingresar por primera vez, el usuario se registre y suministre una serie de datos; cuando usted lo hace, ésta información se almacena en bases de datos y normalmente se comparte con otros sitios de similar preferencia. Si no es vital para su actividad, no proporcione información veraz y cuando lo sea, asegúrese del sitio a quien se le está proporcionando. Alguna información quedará en poder del propietario del sitio (dirección IP, por ejemplo). Incluso algunos sitios Web, podrían vender aquella información.

Hackers

Quiénes son los hackers? La palabra se deriva de hack, término utilizado en inglés para describir las patadas de los jugadores de rugby. Esas mismas patadas eran utilizadas por los técnicos para 'arreglar' las cajas telefónicas y como esa era su función, empezaron a ser llamados hackers.

Hacker es un término usado que se puede interpretar de diversas formas, para algunos los hackers son astutos, intrépidos programadores y para otros, son personas que intentan romper la seguridad de los sistemas computacionales. Luego, cuando ocurrieron las primeras invasiones a la privacidad por vía telefónica, los intrusos heredaron ese nombre; algunos emplean el sobrenombre "pirata informático", pero eso no hace justicia a la idea original.

Para Eric Raymond, compilador del libro The New Hacker's Dictionary, un "good hack" es una inteligente solución a problemas de programación y "hacking" es la acción de realizar tal cosa.

Las siguientes características pueden calificar a un hacker según Raymond:

- "Una persona que disfruta aprendiendo detalles de un lenguaje de programación o sistema y como aprovechar sus posibilidades, al contrario de la mayoría de los usuarios que prefieren aprender sólo lo imprescindible"
- Una persona que disfruta realmente programar; programa en forma entusiasta, casi obsesiva.
- Una persona capaz de apreciar el valor del "hackeo"
- Una persona que programa bien y rápidamente.
- Una persona que es experta en un lenguaje de programación, en un programa en particular o en un sistema operativo.
- Experto o entusiasta de cualquier tipo. Se pude ser un "hacker astrónomo", por ejemplo.
- El que disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.

Liante, malicioso que intenta descubrir información sensible cotilleando por ahí. De ahí vienen "hackers de contraseñas" y "hackers de las redes". El término correcto en estos casos es cracker. Este último término es para aquellos que desean resquebrajar seguridad o realizar actos maldadosos".

Es contra la *ética hacker* alterar datos diferentes a los necesarios para no dejar pistas (logs, etc.). Ellos no necesitan o desean destruir datos como los maliciosos crackers, solo quieren explorar el sistema y conocerlo más, tienen un constante anhelo y sed de conocimiento que se incrementa e intensifica con sus progresos. Dice Gary Robson, de la revista Computers, Security & Internet, "Si llamas hacker

a quien ama la tecnología, a quien tiene conocimiento de cómo ésta trabaja, entonces ya me siento orgulloso y agradecido de ser llamado Hacker". En el medio de los sistemas de información ser llamado hacker es un cumplido, entre la gente común normalmente es un peyorativo.

Termina un hacker inspirado en la constitución o libro de la ley del hacker, realizado por "the mentor, expresando: "Si tener hambre de conocimiento, es ser criminal, si lo soy. Si querer aprender cosas y educarme, o sea, tener acceso a toda la información que necesite, sin tener que pagar por ella, si lo soy; si esto es un crimen, entonces soy un criminal y estoy orgulloso de ello. Nosotros no dañamos a nadie, no fabricamos armas, no traficamos con drogas, nuestro único crimen es la curiosidad y lo que nadie nos perdona es ser más listos que los demás, porque siempre logramos nuestro propósito; pueden detener a uno de nosotros, pero nunca podrán detenernos a todos".

Refiriéndonos a la ética de los hackers, podemos recordar que fue mejor formulada por Steven Levy en 1984, en el libro *Hackers: Heroes of the Computer Revolution*, las principales tesis que esboza son las siguientes:

- "El acceso a las computadoras y a cualquier cosa que pudiera enseñarte algo sobre cómo funciona el mundo, debería ser ilimitado y total.
- Basarse siempre en el imperativo de la práctica.
- Toda la información debería ser libre
- Desconfianza a la autoridad, promover la descentralización.
- Los hackers deberían ser juzgados por sus acciones y habilidades, no por falsos criterios como grados, edad, raza o posición social.
- Se puede crear arte y belleza con la computadora. Las computadoras pueden cambiar tu vida para mejorarla."

CRAKERS

Quienes son los Crackers? El término cracker es otorgado a quien rompe la seguridad de un sistema; fue acuñado hacia 1985 por hackers, en defensa contra la inapropiada utilización del término por parte de periodistas, como: “Es alguien que irrumpe en un sistema de computación, usualmente en una red, desviando o violando claves o licencias en programas de software o en otros casos abre intencionalmente brechas en la seguridad e incluso con propósitos altruistas o por un simple desafío. Algunos rompen, entran y hacen visible los puntos débiles del sistema de seguridad del sitio”.

Para otros, un cracker es quien irrumpe en un sistema violando o adivinando las claves de los usuarios. La mayoría son adolescentes, delincuentes, maliciosos que buscan obtener emoción destruyendo o alterando datos en un sistema. Los crackers tienden a reunirse en grupos pequeños, muy secretos y privados. Algunos crackers a menudo se definen a sí mismos como hackers, la mayor parte de los auténticos hackers los consideran una forma de vida inferior. Por lo tanto, hay mucho menos en común entre el mundo de los hackers y el de los crackers de lo que el lector normal cree, generalmente confundido por el periodismo sensacionalista. **Los hackers se consideran a sí mismos algo así como una elite, en la que los méritos se basan en la habilidad, aunque suelen recibir amablemente a nuevos miembros.**

Entre las variantes de crackers maliciosos están los que realizan **Carding** (Tarjeteo, uso ilegal de tarjetas de crédito), **Trashing** (Basureo, obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos) y **Phreaking** o **Foning** (uso ilegal de las redes telefónicas).

Mecanismos usados por los hackers para acceder a los sistemas informáticos sin autorización.

- **Hurgonear en los basureros.** Hace poco una película basaba toda la estrategia de intromisión informática en encontrar en los basureros físicos de la empresa, las pistas que pudiesen acercarlos con los sujetos a penetrar. A través de la reunión y análisis de los gustos, lugares donde compran, llamadas efectuadas, cuentas de correo de Internet, etc., se puede llegar a conocer la vida de una persona y sus preferencias.
- **Entrar a los sistemas y ejecutar Finger.** Si tengo el nombre de un usuario en un sitio, tengo la mitad de lo que necesito para proceder a realizar mi trabajo, decía un hacker.
- **Usar los servicios de Chat.** Son muchos los hackers que van a estos sitios a buscar usuarios inocentes para "confesarlos" sobre donde trabajan, a que se dedican, averiguan sobre la importancia de la empresa donde laboran y mucho más, localizan sitios que representen para ellos gran interés y generalmente toman la palabra y retan constantemente a los demás, o en algunos casos se hacen pasar por inocentes novatos esperando consejos de alguien que conozca mucho, aplicando lo que se conoce en este medio **como ingeniería social.**

Tomado de:

TAMAYO A., Alonso, DUQUE M., Néstor D. ¿Cómo se deben controlar los sistemas de información?. En: NOOS. Manizales:Universidad Nacional de Colombia. No. 18. 2004. p. 137-147

ANEXO 2

GUÍAS DE LA OCDE PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y REDES

Hacia una cultura de seguridad

OCDE: ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS.

En virtud del artículo I de la Convención firmada el 14 de diciembre de 1960, en París, y que entró en vigor el 30 de septiembre de 1961, la organización para la Cooperación y el Desarrollo Económicos (OCDE) tiene como. Objetivo promover las políticas destinadas:

- A lograr la más fuerte expansión posible de la economía y del empleo y a aumentar el nivel de vida de los países miembros, manteniendo la estabilidad financiera y contribuyendo así al desarrollo de la economía mundial
- A contribuir a una sana expansión económica en los países miembros y no miembros en vías dedesarrollo económico
- A contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria conforme a las obligaciones internacionales.

Los firmantes de la Convención constitutiva de la OCDE son: Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda,

Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia, Suiza y Turquía. Los países siguientes se han adherido posteriormente a esta Convención (las fechas corresponden a las del depósito de los instrumentos de adhesión): Japón (28 de abril de 1964), Finlandia (28 de enero de 1969), Australia (7 de junio de 1971), Nueva Zelanda (29 de mayo de 1973), México (18 de mayo de 1994), República Checa (21 de diciembre de 1995), Hungría (7 de mayo de 1996), Polonia (22 de noviembre de 1996), Corea (12 de diciembre de 1996) y la República Eslovaca (14 de diciembre de 2000). La Comisión de las Comunidades Europeas participa en los trabajos de la OCDE (artículo 13 de la Convención de la OCDE).

Traducido bajo la responsabilidad del Instituto Nacional de Estadística, Geografía e informática (INEGI), México, a partir de las versiones originales en inglés y francés, publicadas respectivamente con los títulos:
OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité © OCDE, 2002

La OCDE no es responsable por la calidad de la traducción al español, ni por su coherencia con el texto original.

Las solicitudes de permiso de reproducción parcial para uso no comercial o destinada a la formación deben dirigirse al Centre Français d'Exploitation du Droit de Copie (CFC), 20 rue des Grands-Agustins, 75006 París, Francia, Tel. (33-1) 44 07 47 70, Fax (33-1) 46 34 67 19, para todos los países excepto Estados Unidos. Para Estados Unidos, la autorización debe obtenerse del Copyright Clearance Center Inc., (CCC) (1- 508) 750-8400,222 Rosewood Drive, Danvers, MA01923 USA, o en CCC Online:

PREFACIO

Desde 1992 cuando la OCDE desarrolló por primera vez las "Guías de seguridad de los sistemas de información a la fecha, se ha presentado un cambio muy dramático en el ambiente general de la tecnología de la información y las comunicaciones, así como en el uso de los sistemas de información y redes. Estos cambios continuos ofrecen grandes ventajas, pero hacen necesario que los gobiernos, los negocios, otras organizaciones y los usuarios que desarrollan, poseen, proporcionan, administran estos servicios y usan sistemas de información y redes (participantes) pongan mayor atención en los aspectos relacionados con la seguridad.

El ambiente que predominaba en el pasado, en el que los sistemas operaban de manera aislada o en redes propietarias, ha sido sustituido por las computadoras personales que cada vez tienen mayor capacidad de proceso, la convergencia de las tecnologías y la difusión masiva del uso del internet. Hoy en día los participantes se encuentran cada vez más interconectados y estas conexiones se extienden más allá de las fronteras nacionales. Al mismo tiempo, el Internet forma parte de la infraestructura de operación de sectores estratégicos como los de energía, transporte y finanzas y desempeña un papel muy importante en la forma en cómo las compañías hacen sus negocios, cómo los gobiernos proporcionan sus servicios a los ciudadanos y a las empresas y cómo los ciudadanos se comunican e intercambian información de manera individual. La naturaleza y el tipo de tecnologías que constituyen la infraestructura de información y

comunicaciones también han cambiado de manera significativa. El número y el tipo de aparatos que integran la infraestructura de acceso se ha multiplicado para incluir dispositivos de tecnología fija, inalámbrica y móvil, y una proporción creciente de los accesos están conectados de manera permanente. Como consecuencia de todos estos cambios la naturaleza, volumen y sensibilidad de la información que se intercambia a través de esta infraestructura se ha incrementado de manera muy significativa.

Como resultado de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente así como un rango de variedad mayor de amenazas y vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad. Por estas razones, estas guías aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor consciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una "cultura de seguridad".

I. HACIA UNA CULTURA DE SEGURIDAD

Estas guías responden a un ambiente de seguridad cada vez más cambiante mediante la promoción del desarrollo de una cultura de seguridad – esto es, un enfoque hacia la seguridad en el desarrollo de sistemas de información y redes, así como la adopción de nuevas formas de pensamiento y comportamiento cuando se usan y se interactúa mediante sistemas de información y redes. Estas guías marcan un rompimiento con los tiempos en que los aspectos de seguridad al desarrollar redes y sistemas se consideraban como un elemento a posteriori. La operación de los sistemas de información, redes y servicios afines debe ser

confiable y segura ya que los participantes se han vuelto cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines puede proveer una seguridad efectiva.

Cada participante es un actor importante para garantizar la seguridad. Cada participante de acuerdo al papel que desempeña deberá estar consciente de los riesgos de la seguridad y de las medidas preventivas correspondientes, deberá asumir la responsabilidad correspondiente y tomar las medidas que permitan fortalecer la seguridad de los sistemas de información y las redes.

La promoción de una cultura de seguridad requiere tanto de un liderazgo fuerte como de una participación amplia para asegurar que se le otorgue un carácter de prioritario a la planeación y administración de la seguridad, así como del entendimiento de la necesidad de seguridad para todos los participantes. Los temas de seguridad deberán ser tópicos de preocupación y responsabilidad para todos los niveles de gobierno, negocios y todos los participantes. Las guías proponen adoptar y promover una cultura de seguridad para toda la sociedad. Esto permitirá que los participantes consideren la seguridad en el diseño y uso de los sistemas de información y de las redes. Las guías proponen que todos los participantes adopten y promuevan una cultura de seguridad como una manera de pensar sobre este tema, así como de evaluar y actuar en relación a los sistemas de información y redes.

II. PROPÓSITOS

Los propósitos de estos lineamientos son:

- Promover una cultura de seguridad entre todos los participantes como un medio de proteger los sistemas de información y las redes.

- Incrementar la concientización sobre el riesgo de los sistemas de información y las redes; las políticas, prácticas, medidas y procedimientos disponibles para poder enfrentar estos riesgos, así como la necesidad de adoptarlos e implementarlos.

- Promover entre todos los participantes una confianza mayor en los sistemas de información y las redes, la forma en la que operan y se usan.

- Crear un marco general de referencia que ayude a los participantes en el entendimiento de los aspectos de seguridad y respeto de valores éticos en el desarrollo e implementación de políticas coherentes, prácticas, medidas y procedimientos para la seguridad de sistemas de información y redes.

- Promover entre todos los participantes cuando sea apropiado, la cooperación y el intercambio de información sobre el desarrollo e implementación de políticas de seguridad, prácticas, medidas y procedimientos.

- Promover la consideración del tema de seguridad como un objetivo importante a lograr por parte de todos los participantes involucrados en el desarrollo e implementación de estándares.

III. PRINCIPIOS

Los siguientes nueve principios son complementarios y deben ser leídos de manera integral. Éstos le competen a todos los participantes de todos los niveles, tanto los del ámbito político como operacional. De acuerdo con estos lineamientos, la responsabilidad de ellos varía de acuerdo con los papeles que desempeñen. Todos se verán beneficiados por la conscientización, educación, intercambio de información y capacitación que conlleven a la adopción de un mejor entendimiento de la seguridad y las prácticas que se requieren. Los esfuerzos para fortalecer la seguridad de los sistemas de información y de las redes deben ser consistentes con los valores de una sociedad democrática, en particular con la necesidad de contar con flujos de información libres y abiertos, y los principios básicos de protección de la privacidad personal.

> *Además de las Guías de seguridad, la OCDE ha desarrollado recomendaciones complementarias concernientes a los lineamientos de otros aspectos importantes de la sociedad de la información mundial. Esto se relaciona con la privacidad (en 1980 las Guías OCDE de Protección a la Privacidad y de los flujos entre fronteras de Datos Personales) y criptografía (la OCDE en 1997 Guía de las Políticas de Criptografía). Las guías de seguridad deben ser leídas de manera conjuntas con ésta.*

1) Conscientización

Los participantes deben estar conscientes de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad.

La conscientización de los riesgos y de los mecanismos disponibles para salvaguardarla, es el primer paso en la defensa de la seguridad de los sistemas de información y redes. Éstos pueden ser afectados tanto por riesgos internos como externos. Los participantes deben entender que las fallas de seguridad pueden repercutir en daños significativos a los sistemas y a las redes que están bajo su control. Deben estar conscientes del daño potencial que esto puede provocar a otros derivados de la interconectividad y la interdependencia. Los participantes deben estar conscientes de: las configuraciones y actualizaciones disponibles para sus sistemas, su lugar dentro de las redes, las mejores prácticas que pueden implementar para fortalecer la seguridad y las necesidades de otros participantes.

2) Responsabilidad

Todos los participantes son responsables de la seguridad de los sistemas de información y redes.

Los participantes que dependen de sistemas de información y redes interconectados de manera local y global deben comprender su responsabilidad en salvaguardar la seguridad de éstos. Deben de responder ante esta responsabilidad de una manera apropiada a su papel individual. Los participantes deben revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular y evaluar si éstos son apropiados en relación a su entorno. Aquellos que desarrollan y diseñan o proveen productos o servicios deben considerar la seguridad de los sistemas y redes y distribuir a los usuarios de manera oportuna información apropiada incluyendo actualizaciones para que éstos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios y la responsabilidad de ellos en relación a este tema.

3) Respuesta

Los participantes deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten la seguridad.

Al reconocer la interconectividad de los sistemas de información y de las redes, así como el riesgo potencial de un daño que se extienda con rapidez y tenga una alcance amplio, los participantes deben actuar de manera oportuna y cooperativa para enfrentar los incidentes que afecten la seguridad. Cuando sea apropiado deben compartir información sobre los riesgos y vulnerabilidades e implementar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten la seguridad. Cuando sea permitido, esto puede implicar el intercambio de información y cooperación transfronteriza.

4) Ética

Los participantes deben respetar los intereses legítimos de los otros.

Debido a la permeabilidad de los sistemas de información y las redes en nuestras sociedades, los participantes necesitan reconocer que sus acciones o la falta de éstas, pueden dañar a otros. Es crucial mantener una conducta ética y los participantes deben hacer esfuerzos por desarrollar y adoptar las mejores prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de otros.

5) Democracia.

La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática.

La seguridad debe ser implementada de manera consistente con los valores reconocidos por las sociedades democráticas, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia.

6) Evaluación del riesgo

Los participantes deben llevar a cabo evaluaciones de riesgo.

La evaluación del riesgo identifica las amenazas y vulnerabilidades y debe ser lo suficientemente amplia para incluir los factores internos y externos fundamentales como tecnología, factores físicos y humanos, políticas y servicios de terceros que tengan implicaciones en la seguridad. La evaluación del riesgo permite determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo de daños potenciales a los sistemas de información y redes, en relación a la naturaleza e importancia de la información que debe ser protegida. Debido a la creciente interconectividad de los sistemas de información, la evaluación del riesgo debe incluir consideraciones acerca del daño potencial que puede ser provocado por otros o que puede ocasionarse a otros.

7) Diseño e implementación de seguridad.

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información y redes.

Los sistemas, las redes y las políticas deben ser diseñados, implementados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo está en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial hacia amenazas o vulnerabilidades que se hayan identificado. Las salvaguardas y mecanismos técnicos y no técnicos son necesarios y deben ser proporcionales al valor de la información de los sistemas de información y redes de la organización. La seguridad debe ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios para sus sistemas.

8) Administración de la seguridad.

Los participantes deben adoptar una visión integral de la administración de la seguridad.

La administración de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debe comprender todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Debe incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención,

detección y respuesta a incidentes que afecten la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoría. Las políticas de seguridad de los sistemas de información, redes, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Los requerimientos en la administración de la seguridad dependen de los niveles de participación, del papel que desempeñan los participantes, del riesgo implicado y de los requerimientos del sistema.

9) Reevaluación

Los participantes deben revisar y reevaluar la seguridad de sus sistemas de información y redes y hacer las modificaciones pertinentes a sus políticas, prácticas, medidas y procedimientos de seguridad.

De manera constante se descubren nuevas amenazas y vulnerabilidades. Los participantes deben revisar y evaluar, modificar todos los aspectos de la seguridad de manera continua, a fin de poder enfrentar los riesgos que se encuentran en evolución permanente.

RECOMENDACIONES DEL CONSEJO DELA OCDE

El Consejo,

Considerando que:

La convención de la organización de la cooperación y desarrollo económicos del 14 de diciembre de 1960, y en particular de los artículos 1 b), 1 c), 3 a) y 5 b) así como

La recomendación del consejo en relación con las guías que regulan la protección de la privacidad y los flujos transfronterizos de datos personales del 23 de septiembre de 1980 (C(80)58/Final);

La declaración sobre flujos transfronterizos de información adoptada por los países miembros de la OCDE el 11 de abril de 1985 (Anexo al C (85)139);

La recomendación del consejo respecto a las guías para políticas de criptografía del 27 de marzo de 1997 (Anexo al C (97)62/Final);

La declaración ministerial sobre la protección de la privacidad en las redes globales del 7-9 de diciembre de 1998 (Anexo al C (98)177/Final)

La declaración ministerial sobre la autentificación del comercio electrónico del 7-9 de diciembre de 1998 (Anexo al C (98)177/Final);

Y reconociendo:

Que los sistemas de información y redes son cada vez más usados y de un valor creciente para los gobiernos, las empresas y otras organizaciones, así como los usuarios individuales;

Que la creciente importancia del papel de los sistemas de información y redes y la creciente dependencia en ellos para asegurar la estabilidad y eficiencia de las economías nacionales y del comercio internacional, y de la vida social, cultural y política, hacen evidente la necesidad de desarrollar esfuerzos especiales para proteger y promover la confianza en ellos;

Que los sistemas de información y redes y su proliferación en todo el mundo han estado acompañados de nuevos y crecientes riesgos;

Que los datos e información almacenados y transmitidos a través de los sistemas de información y redes están sujetos a amenazas de accesos, usos, apropiación y alteración no autorizados, transmisión de código dañino, caída o destrucción del servicio, y requieren de mecanismos adecuados para salvaguardarlos;

Que existe la necesidad de incrementar la conscientización sobre los riesgos a los sistemas de información y redes, y de las políticas, prácticas, medidas y procedimientos disponibles para responder a éstos, y que promover un comportamiento adecuado como un paso esencial para el desarrollo de una cultura de seguridad;

Que hay una necesidad de revisar las políticas, prácticas, medidas y procedimientos con los que se cuentan en la actualidad para ayudar a asegurar

que éstos sean capaces de responder a los retos cambiantes de las amenazas que enfrentan los sistemas de información y redes;

Que es del interés común promover la seguridad de los sistemas de información y redes mediante una cultura de seguridad que promueva la coordinación y cooperación internacional para enfrentar los riesgos para las economías nacionales, el comercio internacional y la vida social, cultural y política provocados por el daño potencial de fallas en la seguridad.

Reconociendo también:
Que las *Guías para la seguridad de los sistemas de información y Redes: Hacia una cultura de seguridad* puestas en este anexo son recomendaciones de carácter voluntario y no afectan los derechos de la soberanía de las naciones;

Que estas guías por ningún motivo sugieren que exista una solución única para la seguridad o qué políticas, prácticas, medidas y procedimientos son apropiados para una situación particular, sino más bien, buscan proveer un marco de principios para promover una mejor comprensión de cómo los participantes pueden beneficiarse y contribuir al desarrollo de una cultura de seguridad;

Recomienda estas *Guías para la seguridad de los sistemas de información y Redes: Hacia una cultura de seguridad* a gobiernos, empresas, otras organizaciones y usuarios individuales que desarrollen, posean, provean, administren o proporcionen servicio y usen sistemas de información y redes.

Recomienda a los Países Miembros:
Establecer nuevas o modificar las políticas, prácticas, medidas y procedimientos con que cuenten para reflejar y tomar en cuenta el contenido de las *Guías para la*

seguridad de los sistemas de información y Redes: Hacia una cultura de seguridad mediante la adopción y promoción de una cultura de seguridad como
proponen estas guías;

Desarrollar esfuerzos para consultar, coordinar y cooperar a nivel nacional e internacional a efecto de poder implantar estas guías;

Dar a conocer las guías al sector público y privado, incluyendo las organizaciones de los gobiernos, los negocios y otras y usuarios individuales para promover una cultura de seguridad y hacer que todas las partes involucradas respondan a este llamado, desarrollen las acciones necesarias para implementar estas guías de una manera adecuada a sus papeles individuales;

Poner a disposición de países no miembros estas guías en el tiempo y forma adecuados;

Revisar estas guías cada cinco años para promover la cooperación internacional en aspectos relacionados con la seguridad de los sistemas de información y las redes;

Instruye al Comité de Política de información, Computación y Comunicaciones de la OCDE para promover la implantación de estas guías.

Esta recomendación sustituye la recomendación del consejo concernientes a las guías de seguridad de los sistemas de información del 26 de noviembre de 1992 (C(92)188/Final). GUÍAS DE LA OCDE PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y REDES
12 © OECD 2002

ANEXO 3

ISO/IEC 27000-series

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene 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). la mayoría de estas normas se encuentran en preparación e incluyen:

ISO/IEC 27000 - Es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.

ISO/IEC 27001 - Es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estandar internacional en octubre 2005.

ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la

información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 01 de julio de 2007.

ISO/IEC 27003 - Son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Se encuentra preparación y probablemente sea publicada en 2009.

ISO/IEC 27004 - Son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Se encuentra preparación y probablemente sea publicada en 2009.

ISO/IEC 27005 - Trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de seguridad en la información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en Junio de 2008.

ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

*** ISO/IEC 27007 -** Es una guía para auditar al SGSI. Se encuentra en preparación.