¿Cómo construir la cultura de manejo y respeto de la información digital en los funcionarios de las Fuerzas Militares?

Sonia Dolly Gutierrez Carrillo
Pedro Martín Barros Barrios

Trabajo de grado para optar al título profesional:
Curso de Información Militar (CIM)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2007

FUERZAS MILITARES DE COLOMBIA

ESCUELA SUPERIOR DE GUERRA

TRABAJO DE FUERZA

¿CÓMO CONSTRUIR LA CULTURA DE MANEJO Y RESPETO DE LA INFORMACIÓN DIGITAL EN LOS FUNCIONARIOS DE LAS FUERZAS MILITARES?

MY. SONIA DOLLY GUTIÉRREZ CARRILLO
MY. PEDRO MARTÍN BARROS BARRIOS

Curso CIM-2007

Bogotá DC.

16 de Abril de 2007

Nota de aceptación:

Excelente trabajo; de gran aplicación para las FF.MM., en desarrollo de la DP. 200-12/2006 "Políticas de Seguridad Informática para las FF.MM".
Esta Metodología, se debe implementar de manera inmediata, con el apoyo de campañas y acciones orientadas por los oficiales del Sistema de Gestión de Seguridad de la Información y los Ofles de Seguridad Informática de las Fuerzas.

CN. Marco F. Gélvez A.

Firma del presidente del jurado

CR Julian Zuluaga

Firma del jurado

Firma del jurado

Bogotá, 16 de Abril de 2007

RESUMEN

Título de la investigación: Construcción de cultura de manejo y respeto de la información digital en los funcionarios de las fuerzas militares.

Investigadores: MY. SONIA DOLLY GUTIÉRREZ CARRILLO
MY. PEDRO MARTÍN BARROS BARRIOS

Problema Formulado: ¿Cómo construir la cultura de manejo y respeto de la información digital en los funcionarios de las fuerzas militares?

Objetivo general: Proponer políticas y estrategias para modificar la cultura organizacional en el manejo de la información en las Fuerzas Militares, tendientes a garantizar que cada funcionario aplique Políticas y Estándares de Seguridad; y entienda su rol y responsabilidad en la protección de la información.

Tipo de investigación: Documental

Síntesis de los resultados encontrados: La Institución Militar debe incrementar sus esfuerzos en crear una cultura de respeto, protección y seguridad de la información basado en estrategias y políticas, iniciando a través de un plan de concienciación para cautivar y motivar a todos los funcionarios con el fin de evitar la generación de errores, pérdida o fuga en la manipulación de la información, toda vez que con un mal uso o descuido se pueden afectar la credibilidad ciudadana, moral de las tropas y el cumplimiento de la misión constitucional.

Palabras clave: Concienciación para la protección y respeto a la información

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

Las personas son necesarias e irremplazables para el funcionamiento de los sistemas informáticos, deben ser consideradas como parte integrante de estos, y por tanto han de concebirse auténticas normas de seguridad que tengan en cuenta su actuar y pensar.

Las Fuerzas Militares deben poder conocer y controlar el uso de los recursos informáticos por parte de su personal, la sola previsión de los aspectos tecnológicos de la seguridad no bastan para garantizar el uso y la seguridad adecuada de la información digital, se requiere definir estrategias, políticas y procesos para modificar la cultura organizacional en este campo.

El Ministerio de Defensa y las Fuerzas hasta la fecha han emitido resoluciones, directivas y otros tipos de normatividad sobre el correcto uso de los medios informáticos, sin embargo estos no son suficientes para lograr crear una conciencia sobre el adecuado uso y protección de la información digital.

El alcance de esta monografía investigativa es formular políticas, estrategias y recomendaciones para crear una cultura de seguridad informática en los funcionarios de las Fuerzas Militares, con base en el marco teórico de lo que son las estrategias y políticas informáticas, cultura organizacional y la experiencia como Ingenieros de Sistemas e interacción con los usuarios por parte de los autores.

Para el desarrollo de este trabajo se describe en el primer capítulo la forma general como los funcionarios públicos de las Fuerzas Militares manejan la información y los equipos de telemática.

En el segundo capítulo se plantea la importancia de definir mecanismos de seguridad para la información digital, así como las características y condiciones que deben salvaguardarse para los datos y sistemas informáticos. Adicionalmente, se describen los estándares internacionales que existen en el tema de seguridad informática, el marco teórico y recomendaciones para la formulación de las "estrategias" que debe asumir una organización en pro de una cultura de seguridad informática.

El tercer capítulo se centra en la importancia de la definición de las políticas de seguridad informática, las cuales son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base del plan maestro para la implantación efectiva de medidas de protección. Al final de este segmento de la monografía se formulan políticas para la identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos, entre otros.

El cuarto capítulo corresponde al marco referencial que igualmente era uno de los resultados esperados del trabajo, cómo construir un marco teórico - conceptual para los proyectos de concienciación y en este estudio con énfasis en Seguridad de la Información, evaluándolo como parte de los procesos de Gestión Humana, Tecnología de la Información, Cultura Organizacional y la Seguridad de la Información. Por último llegar al Modelo propuesto resultado de este estudio, que integra los sistemas mencionados anteriormente, y concluye en una propuesta de awareness para cautivar la atención de los funcionarios de las FF.MM. en el tema de la seguridad informática, que posteriormente facilite la conversión de los deberes en hábitos, a través de cambios en las percepciones personales de los deberes que emergen del proceso de seguridad de la información, buscando la identificación con la Cultura Corporativa.

El proceso de Concienciación para promover la seguridad de la información dentro de los funcionarios de las Fuerzas Militares, se basa en la elaboración del

Programa de Concienciación de la Protección de Información (PCPI), Se definen los siguientes dos objetivos principales: Asegurar que cada empleado o área de las FF.MM. aplique las Políticas y Estándares de Seguridad y asegurar que cada funcionario de las FF.MM. entienda su rol y responsabilidad en la protección de la información.

El último capítulo son las conclusiones y recomendaciones, resultado de la experiencia vivida en la recopilación de las ideas y los conceptos trabajados en la investigación y plasmados en este documento.

1. JUSTIFICACIÓN

A pesar de que el Código Penal en su Artículo 418 "Revelación del Secreto" establece: "El servidor público que indebidamente de a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en multa y perdida del cargo, si de la conducta resultare perjudicada la Institución, la pena será de uno (1) a tres (3) años de prisión, multa de quince (15) a sesenta (60) salarios mínimos legales mensuales vigentes e inhabilitación para el ejercicio de derechos y funciones públicas por cinco (5) años"; se siguen presentando hechos y sucesos que en algunas oportunidades han generado hallazgos de información confidencial, reservada, secreta o de propiedad de las Fuerzas Militares tanto en personas como en lugares equivocados, tal como el caso "del hallazgo de información de la organización y dotación de una dependencia militar en el equipo de cómputo portátil de un señor profesor de una Universidad Pública, a quien sin ninguna intensión de daño o perjuicio se le entregó información".

Aunque existe un marco que sanciona el uso indebido de la información, mencionado anteriormente, es necesario generar un enfoque que vaya más allá de lo únicamente punitivo, se debe desarrollar una estrategia integral de manejo y uso de la información por medio de la construcción de una cultura de respeto de la información digital.

La no existencia de una cultura organizacional que defina las implicaciones, responsabilidad y riesgos que tiene el uso de la información es crítico para el medio militar, toda vez que la situación de conflicto que vive el país le acrecienta su importancia para el logro de la paz, bien común y desarrollo del país.

Por lo anterior, se hace necesario que la Institución desarrolle unas políticas y estrategias claras para proteger, controlar el uso y flujo de la información,

inmersas en una nueva cultura organizacional, de tal forma que los esfuerzos y actividades de las FF.MM. se concentren en las operaciones contra los grupos enemigos y no en la custodia, vigilancia, control y solución de errores técnicos, administrativos y de comportamiento del ser humano con el manejo incorrecto de la información.

2. PLANTEAMIENTO DEL PROBLEMA

La información cada día es más crítica y vital para el cumplimiento de la misión y funciones asignadas a las Fuerzas Militares, en la actualidad se considera como un activo más de cualquier tipo de organización, por tal razón cada entidad debe extender el proceso de "Gestión" a la información.

Al ser la información un recurso, se hace necesario replantear la cultura organizacional a través de la formulación de nuevas políticas, estrategias y mecanismos para la protección, uso y manejo de la información, tendientes a evitar la fuga, el empleo indebido, pérdida, modificación parcial o total, así como el acceso indiscriminado a la información confidencial e información sensible por parte del personal no autorizado; dichas actividades cobran mayor valor si se considera el nuevo contexto tecnológico en el que se obtiene, procesa, difunde y archiva la información en la Institución Militar Colombiana en la actualidad.

El uso generalizado de la información en condición digital en las FF.MM. genera mayores riesgos, accidentes y la hace más asequible y apetecible por los agentes generadores de violencia que atentan contra la seguridad y democracia del país, dada su "facilidad" de obtención en tiempo y sin importar la ubicación; lo anterior demuestra una vez más la importancia que reviste establecer políticas y estrategias que orienten el comportamiento de los funcionarios públicos con la administración, procesamiento, utilización y protección de la información.

2.1 FORMULACIÓN DEL PROBLEMA

¿Cómo construir la cultura de manejo y respeto de la información digital en los funcionarios de las Fuerzas Militares?

2.2 OBJETIVO GENERAL

Proponer políticas y estrategias para modificar la cultura organizacional en el manejo de la información en las Fuerzas Militares, tendientes a garantizar que cada funcionario aplique Políticas y Estándares de Seguridad; y entienda su rol y responsabilidad en la protección de la información.

2.3 OBJETIVOS ESPECÍFICOS

2.3.1. Evaluar el manejo que se le da a la información por parte de los funcionarios de la FF.MM (Oficiales, Suboficiales, Soldados y Personal civil).

2.3.2 Recomendar estrategias, políticas de protección y estándares de seguridad contra el riesgo informático.

2.3.3 Plantear mecanismos para interiorizar las políticas de seguridad de la información, utilizando herramientas para la distribución, educación y cumplimiento de políticas.

2.3.4 Formular políticas de protección y estándares de seguridad que le permitan a las FF.MM generar hábitos de seguridad informática en todos sus funcionarios.

2.3.5 Identificar el concepto, componentes y herramientas para la generación y/o modificación de una cultura organizacional.

3. CÓMO SE MANEJA LA INFORMACIÓN EN LAS FF.MM.

A continuación, se describe la forma como se maneja la información tanto en el área operacional como en el área administrativa en las Fuerzas Militares, para ello se establecerán conceptos de dos (2) tipos de información: *Información Digitalizada,* la cual es aquella que se realiza apoyada en el computador, es decir que reside en dispositivos de medio electrónico, como son el disco duro, diskettes y memorias, entre otros.

El segundo es la *Información No Digitalizada* la cual se refiere a todo documento físico que fluye durante el desarrollo de una determinada tarea específica; llámense oficios, radios, memorandos, circulares y resoluciones, entre otros; que para el caso de la presente monografía no se evaluará, solo se analizará el aspecto de la información digitalizada.

3.1 ANTECEDENTES

Basados en el conocimiento y experiencia laboral se establece que en el último cuatrienio el desarrollo tecnológico de las Fuerza Militares, se ha convertido en una de las estructuras pilares que sirve de apoyo para el cumplimiento de las funciones y el logro de los objetivos estratégicos propios y de las entidades con que interactúa cada dependencia militar, como son el Ejército Nacional, Armada Nacional, Fuerza Aérea, Comando General de las FF.MM. y la Secretaria General del Ministerio de Defensa.

Para ello se ha adquirido software y equipos de cómputo de última generación para todos los niveles de la organización (altos mandos, mandos medios y

usuarios finales), y se ha desarrollado una infraestructura de red de datos y comunicaciones a nivel nacional que permite el cumplimiento de las tareas administrativas y operativas de la Institución de manera más ágil, sencilla y estructurada.

Sin embargo, el hecho de que el personal de la Institución cuente con equipos de cómputo conectados en red y software de última tecnología, con altos componentes y esquemas de seguridad propios de fábrica, no se garantiza que su operatividad sea totalmente segura al realizar las labores propias del trabajo de cada funcionario.

Por lo contrario se percibe un comportamiento desinteresado, muchas veces descuidado por parte de los usuarios con el activo más importante para la Institución en esta época, como lo es "la información" que se maneja en todas las áreas funcionales de la organización; varias veces tal actitud ha generado sucesos de riesgo en el área informática, resultado de la propagación de virus, gusanos y spam, intensificados con el uso del correo y el acceso indebido al Internet .

Cómo partícipes del proceso de interacción con los usuarios finales en el área tecnológica de la Fuerzas Militares se identifica que en la Institución Castrense, es común encontrar pensamientos y actitudes como los que se describen a continuación:

- Todas las fallas no serán notorias en forma inmediata.
- Lo que hacemos no es importante.
- Las personas de las Oficinas de Tecnologías de Información y del Centro de Cómputo saben qué hacer ante una emergencia.
- Es fácil conseguir los elementos de reemplazo, no hay necesidad de exagerar en los cuidados (insumos, aire condicionado, servidores, discos, etc.)

- Los clientes internos y otros receptores de los servicios van a entender si hay fallas y errores.
- Los sistemas de alarma son infalibles.
- Con la UPS y el Firewall es suficiente para proteger los sistemas informáticos.
- A nosotros no nos va a suceder; otro día hago copias de seguridad.
- Los procedimientos de auditoria y control son responsabilidad del personal del centro de computo y no del usuario.
- Se cuentan con dispositivos de seguridad física para los computadores y los sistemas no pueden ser violados si no se ingresa al centro al centro de cómputo, ya que no se considera el uso de terminales y de sistemas remotos.
- En los casos de seguridad que tratan de seguridad de incendio o robo; que "eso no me puede suceder a mí" ó "es poco probable que suceda".
- Los computadores y los programas son tan complejos, que nadie fuera de la Institución los va a entender y no les van a servir, ignorando las personas que puedan captar y usarla para otros fines.
- Los sistemas de seguridad generalmente no consideran la posibilidad de fraude interno que es cometido por el mismo personal en el desarrollo de sus funciones.
- La seguridad por clave de acceso es inviolable pero no se considera a los delincuentes sofisticados.
- Se suele suponer que los defectos y errores son inevitables.
- También se cree que ocurren fallas porque nada es perfecto.
- Y la creencia que la seguridad se aumenta solo con la inspección o sólo es responsabilidad del personal del área informática.

Estos hechos anteriormente citados suceden y son mucho más frecuentes de lo que se supone. No siempre los problemas toman una dimensión pública porque

suelen ocultarse y no se denuncian los incidentes de seguridad. Esta actitud empeora las cosas porque los casos no se documentan y permiten que causas que produjeron el problema queden latentes y el incidente pueda repetirse.

Es comúnmente difundido, que lo que no se puede medir no se puede mejorar y es mucho más problemático en el campo de seguridad de la información, la existencia de una falsa percepción de la seguridad. Esto hace difícil medir y poner parámetros al estado real de la información además de proyectar cambios alineados con un proyecto de mejora. Por ello, la institución castrense a través de la Directiva Permanente No. 200-12 del 29 de diciembre de 2006, emite una serie de órdenes con el fin de dar inicio a la conformación de una estructura organizacional para la gestión de la seguridad de la información a nivel FF.MM.

Como se dijo anteriormente, y soportados en la experiencia en la Institución se percibe una carencia de responsabilidad con el cuidado y respaldo de la información; tal es así, que a diario se presentan casos de negligencia, ya que se dejan computadores totalmente desprotegidos sin ninguna contraseña, o cuando existe la contraseña fácilmente la dejan anotada en lugares visibles, donde cualquier persona puede llegar e ingresar al sistema para copiar, alterar o en muchos casos sustraer la información sin el conocimiento del dueño o responsable directo.

Este tipo de eventos en el área administrativa generan preocupación en el momento de cumplir con las obligaciones fiscales y de control ante los diferentes entes tanto internos como externos como son: la Dirección de Impuestos Nacionales, el Ministerio de Hacienda y Crédito Público, Contraloría, Contaduría General de la Nación, Dirección de Finazas del MDN y Oficina de Control Interno, toda vez que ante la situación de incumplimiento de los plazos o entrega de información financiera distorsionada por parte de la Institución a los organismos de control o directores se ve abocada a pagar multas o ser sancionada y puede ser

reportada a las diferentes entidades de control por el incumplimiento de las normas.

Sin embargo, el área operativa no se escapa de este manejo que le dan los usuarios, a pesar de que existe un grado mayor de cuidado por la información y que en algunas dependencias se cuenta con niveles físicos de seguridad como control de acceso, a nivel biométrico, cámaras de vigilancia etc., y que en muchos de estos sitios se requisan bolsos, maletines, paquetes, etc., se peca porque la información operacional puede viajar a través de los correos gratuitos proveídos por el Internet, de las memorias USB, de los equipos portátiles personales, teléfonos, cámaras digitales, entre otros.

Es así como en muchos de los hallazgos y requisas hechos durante los retenes se han encontrado equipos portátiles con información que hace referencia al desarrollo completo de operaciones militares, capacidades, recursos y datos del personal de la Institución.

La razón de lo anterior, no es más sino una, y es que en la medida que evolucionan las tecnologías informáticas, se incrementa la necesidad de plantear esquemas claros de protección sobre la información; tal esquema debe enmarcarse dentro del contexto de una metodología de seguridad que trabaje sobre los principios básicos de seguridad como son: la autenticación, confidencialidad, integridad, disponibilidad, control de acceso y auditoría.

La cultura de seguridad de la infraestructura de informática que se ha venido creando en la Institución, se basa en proteger las redes con Firewall, Proxy y mantener un buen antivirus actualizado en los equipos de cómputo, pero eso no es todo.

La seguridad informática es un área que día a día exige la presencia de un equipo humano capacitado y dedicado a esta labor, lo que ha conllevado a la especialización de estas personas en diversos campos de la seguridad informática.[1]

La necesidad de que al interior de la Institución se genere una cultura enfocada a la seguridad permite desarrollar esquemas de control de una forma más participativa, rápida y eficiente. Para llegar a desarrollar una cultura en seguridad informática, es necesario velar porque las políticas de seguridad se transmitan a todas los funcionarios de la Institución, además de contar con el apoyo del alto mando.

En general, se observa que en el manejo de la información en las Fuerzas, no basta con tener grandes avances de tecnología sino que también se requiere conocer, en manos de quién está esta tecnología. No hay sistema de protección que sea infalible cuando es manejado por seres humanos.

La experiencia y cantidad de sucesos que se presentan a diario, demuestran que los datos se pierden en infinidad de maneras, ya sea por un simple accidente o como resultado de un error de usuario.

Para una mayor claridad de lo que ocurre con el manejo de información en la Institución, se observa por ejemplo que: el contenido de un libro, canción, imagen, video, documento, etc. puede transformarse en un archivo digital utilizando una computadora. En otras palabras, es posible copiar la información almacenada en formato tradicional a un formato digital y, en consecuencia, utilizar un equipo de cómputo para manipular (i.e. reproducir, modificar, consultar, enviar, etc.) dicha información digitalizada.

---

[1] HUERTAS, Juan Carlos. Seguridad Corporativa. Revista Sistemas No. 77 p.50

La ventaja de usar el archivo digitalizado en lugar del formato original (documento), radica en la rapidez y facilidad con que se puede manipular dicha información. Para la institución el hecho de que se tenga la información digitalizada le facilita tomar decisiones en forma oportuna; un caso que ilustra esta situación, es la forma como se realiza este proceso en el desarrollo de las operaciones militares, ya que la información se tiene en tiempo real, precisamente por tener la propiedad de que está digitalizada y si es así, también cumple con la característica de oportunidad y obviamente de veracidad. Todo esto permite a la Institución tener éxito en las misiones, ya que la materia prima con que realiza tales tareas es la información digitalizada en la gran mayoría de los casos.

Debido a estas ventajas, la digitalización de la información se aplica cada vez en más áreas de la Organización, por ejemplo en la Fuerza Aérea se observa en el ámbito operativo con la digitalización de los manuales y boletines técnicos de las diferentes aeronaves que le permiten al personal técnico en un momento determinado tomar las decisiones de una manera ágil y oportuna en el mantenimiento y reparación de las mismas. Lo mismo se observa en el área de contratos, manejo y archivo de folios de vida y otra documentación Institucional.

El personal del área de tecnologías de información de la Institución considera que el crecimiento de la información digitalizada se ha intensificado desde la aparición de Internet, aspecto que permite que pueda ser enviada a cualquier otro equipo de cómputo conectado a Internet en cualquier parte del mundo a un costo muy bajo.

Esta es la razón por la cual en el ambiente informático de comunicaciones se dice que con Internet los equipos de cómputo se han transformado en los teléfonos del siglo 21, ya que antes los empleados de la Institución utilizaban el teléfono para poder intercambiar sonidos y datos con otras personas en el mundo, hoy en muchos casos esos mismos funcionarios de la organización pueden utilizar equipos de cómputo para intercambiar cualquier tipo de información enriquecida

en archivos digitales (texto, sonidos, imágenes, videos, etc.) con cualquier persona en el mundo conectada a Internet o a una red de cómputo.

Lo anterior es una facilidad muy acertada y útil siempre y cuando se realice con seguridad, y es ahí donde se comenten errores porque en muchas oportunidades no se tiene cuidado en la transferencia de información, ya que existe un desconocimiento profundo por parte de los funcionarios de la Institución, en cuanto a que el mundo de Internet ***no es seguro;*** genera bondades, pero no garantiza lo más importante para una entidad castrense, dado que en la red se pueden capturar, modificar y desviar los datos, entre otros; por lo tanto se corre el riesgo de perder la confiabilidad e integridad de la información.

Las Fuerzas Militares reconocen que la información digitalizada es más beneficiosa, ya que dispone de una mayor *preponderancia* que la información en formato "tradicional" y sus ventajas inherentes hacen que su uso se siga extendiendo. Por ello la Institución durante los últimos años ha realizado grandes esfuerzos por desarrollar una infraestructura tecnológica que le permite utilizar las bondades de la información digitalizada, por lo que en el transcurso del tiempo, el uso de los equipos de cómputo se ha ido incrementando en las diferentes unidades tanto operativas como administrativas, al punto que, en el día de hoy, las Fuerzas dependen de esta tecnología para poder funcionar en condiciones normales.

La infraestructura tecnológica actual obedece a la vertiginosa velocidad con que van evolucionando las tecnologías informáticas y de comunicaciones, generando un desafío sin precedentes al momento de garantizar la preservación de un nuevo activo como lo es la información y en esto la Institución Castrense no se puede quedar replegada. Hoy en día se requiere para ser competitivo que se adquiera un nivel tecnológico seguro; de lo contrario, la Institución desconocerá y desaprovechará el valor agregado de la información confiable y oportuna.

Pero también se puede evidenciar que los riesgos que ha afrontado la Institución durante los últimos años son consecuencia de estar montada en el bus del "avance tecnológico" sin las adecuadas tecnologías de seguridad y procedimientos defensivos. Los hackers, ingeniería social, ciberterrorismo, robo de información, virus, negación de servicio, troyanos, phishing, incendios, sabotajes, catástrofes y otras contingencias acechan todos los días conspirando contra el tiempo disponible de los sistemas, vitales para la entidad castrense que debe cumplir lo establecido en la Constitución Nacional para la defensa de la seguridad y soberanía nacional, actividad que se ejerce durante las 24 horas del día, los siete días de la semana; más aún cuando el éxito de las operaciones militares requiere de una materia prima como es la información oportuna, confiable e íntegra.

En la actualidad se han hecho esfuerzos a nivel de cada una de las fuerzas y del mismo Ministerio de Defensa para expedir resoluciones, decretos y directivas, entre otros, que hacen referencia a la normatividad que debe regir el *uso correcto de los recursos informáticos*; sin embargo, estas medidas no son suficientes ya que carecen de una etapa de divulgación de lo que se pretende con ello, y muchas veces no se explica a la totalidad de los funcionarios, cual es el objetivo que se pretende con ello. No existe una verificación de que se esté cumpliendo permanentemente con estas medidas, y en varias ocasiones estos documentos quedan archivados, sin realizarse ningún tipo de seguimiento y control, y mucho menos no se realiza actualización del documento, quedando a veces como unas medidas obsoletas.

Por todo lo anterior, la Institución debe incrementar sus esfuerzos en crear un plan de concienciación de la seguridad y protección de la información y evitar la generación de errores, pérdida o fuga en la manipulación de la información ya que con esto se podría afectar de manera significativa la "Credibilidad Ciudadana", moral de las tropas y cumplimiento de la misión constitucional; por esto, la

Institución debe trabajar diariamente sobre un proceso de mejoramiento continuo de la cultura de la seguridad de la información.

4. POR QUÉ EL INTERÉS DE IMPLEMENTAR MECANISMOS SEGURIDAD INFORMÁTICA EN LA INSTITUCIÓN

Luego de haber realizado una breve descripción del manejo de la información en la Institución, y con el fin de que no se pierda el hilo conductor en este capítulo que hace referencia a "*Políticas y Estrategias de la información*", a continuación se describe la importancia de generar normas de seguridad informática.

Como se indicó anteriormente, el actual desarrollo tecnológico, en el cual se soporta la Institución, ha convertido las estructuras informáticas en uno de los más importantes factores críticos de éxito para el logro de los objetivos estratégicos. Sin embargo, se requiere que la infraestructura tecnológica esté acompañada de unos lineamientos, normas, políticas y lo más importante, de una cultura informática que le permita conducir a la Organización a un nivel de madurez en el campo de la seguridad de la información. De no lograrlo quedaría aislado por no ser un ente competitivo. Por ello, es importante resaltar que la seguridad informática requiere el compromiso de todos los funcionarios de los diferentes niveles de las Fuerzas Militares.

4.1 SEGURIDAD DE LA INFORMACIÓN

La información no es estática, esto significa que alcanzan el mismo grado de importancia tanto la capacidad de transmitir en sentido bilateral, como la capacidad de emitir o recibir a través de las redes globales en forma segura.

La seguridad de la información se logra mediante la implantación de un conjunto adecuado de controles que abarca políticas, prácticas, procedimientos, estructuras

organizativas y funciones de software que aseguran una garantía razonable o suficiente de que se lograrán los objetivos de la Institución[2] así como con la actitud positiva del factor humano en cuanto a su aplicación y cumplimiento.

Por lo tanto, la seguridad de la información protege a la Institución de una amplia gama de amenazas, a fin de garantizar la continuidad de la Organización, minimizar el daño a la misma y maximizar el cumplimiento de los objetivos y de las oportunidades.

Se puede entender la seguridad de la información a través de las siguientes características:

- **Confidencialidad:** garantiza que la información sea accesible sólo a funcionarios de la Institución autorizadas a tener acceso a ella.

- **Integridad:** salvaguarda la exactitud y totalidad de la información y sus métodos de procesamiento y comunicación. Debe contener en forma completa lo que se espera que contenga. También implica que la información que se recibe en un punto remoto de una red debe ser exactamente igual a la que se emitió en un punto local.

- **Disponibilidad:** garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, en el momento que se requiera y donde se requiera.

Adicionalmente, deberán considerarse los conceptos de:

---

[2] GARCIA,Gustavo. Un mundo de Cambios. Revista tecnología de información enero-febrero 2007 p.67

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente documento, se realizan las siguientes definiciones:

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la Información**: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

4.1.1 Amenazas deliberadas a la seguridad de la información. Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos permiten identificar las amenazas que han de ser contrarrestadas.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino, como por ejemplo otro archivo o un usuario. Un ataque no es más que la materialización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- **Interrupción**: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son: la destrucción de un elemento

de hardware, como un disco duro; cortar una línea de comunicación ó deshabilitar el sistema de gestión de ficheros.

- **Interceptación**: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un computador. Ejemplos de este ataque son: pinchar una línea para hacerse con datos que circulen por la red, la copia ilícita de archivos o programas (interceptación de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (interceptación de identidad).

- **Modificación**: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos; alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- **Fabricación**: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico; una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- **Control del volumen de tráfico** intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

4.1.1.2 Ataques activos. Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos

privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de **negación de servicio**, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc. [3]

[3] http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html 09-Mar-07

4.2 LEGISLACIONES ACTUALES

Existe un grupo de nuevas leyes que hacen legalmente responsables a los Directivos de cualquier tipo de empresas si no protegen sus activos de información bajo amenaza de sanción. La responsabilidad está en promover el interés y la prudencia necesaria en evaluar el riesgo y determinar las medidas pertinentes para reducirlo o eliminarlo.[4]

A partir de los escándalos fiscales de Enron, Global Crossing y World.Com, fruto de los defectos y lagunas de los sistemas de información empresarial financiera, la ley estadounidense Sarbanes-Oxley Act, conocida como SOX, se desarrolló teniendo como objetivo generar un marco de transparencia para las actividades y reportes financieros de las empresas que cotizan en bolsa, y darle mayor certidumbre y confianza a inversionistas y al propio estado.

SOX contempla una revisión más rigurosa de los datos que los que una empresa declara en sus estados financiero–contables y de los que utiliza para sus controles internos. Esto no solamente abarca fraudes por falsedad en dichas declaraciones, sino también por inferencia y todos los casos de fraude en los que se desvirtúen de manera importante los estados financieros, como la malversación de activos y actos de corrupción, entre otros. Las multas por proveer información falsa o incorrecta son muy severas y pueden llegar al extremo de encarcelar a los ejecutivos de la empresa o que ésta sea retirada de la bolsa de valores en que cotiza.

---

[4] GARCIA,Gustavo. Un mundo de Cambios. Revista tecnología de información. Enero-Febrero 2007 p.68

4.3 GESTIÓN DE SEGURIDAD Y NORMAS APLICABLES

Dado que mantener la seguridad es un problema y algo hay que hacer para solucionarlo, lo mejor es hacerlo teniendo en cuenta la guía de normas internacionales aplicables. No hace falta inventar la rueda, alguien lo hizo antes. Por esto la Institución se debe centrar en la implementación de dichos estándares y capacitación.

Entre las principales normas y metodologías podemos citar:

- Information Systems and Audit Control Association – ISACA:
- COBIT
- ITIL (IT Infrastructure Library)
- British Standards Institute: BS 7799
- International Organization for Standarization: Normas ISO
- Departamento de Defensa de los Estados Unidos: Orange Book / Common
- Criteria
- ITSEC – Information Technology Security Evaluation Criteria:
- White Book
- Sans Institute, Security Focus
- Sarbanes Oxley Act, Basilea II, HIPAA Act,
- ISO17799:2005, ISO27001

Entre todas estas, la última es la que se va perfilando como un estándar de aplicación universal.

La Norma ISO 17799:2005 denominada Código de Práctica para la Administración de la Seguridad de la Información, es un estándar internacional de seguridad que

provee las mejores prácticas para la definición de controles, proporcionando proactivamente soluciones para evitar interrupciones en las actividades y procesos del negocio, asegurando una protección adecuada para los sistemas de información contra amenazas internas y externas.[5] Ver Figura 1.

Esta norma no es certificable ya que se trata de recomendaciones. Para hacer una certificación deberá hacerse sobre la Norma BS 7799 parte 2 denominada "Sistemas de gestión de la seguridad de la información". Cabe destacar que bajo los lineamientos de ISO, la última actualización de esta norma se ha transformado en la ISO 27001 denominándose:

Information Technology - Security Techniques – Information Security Management Systems – Requirements. La cual está conformada por diez secciones, tratando la primera parte los controles y la segunda la certificación del SGSI o Sistema de gestión de seguridad de la información.

La seguridad no es un proyecto sino un proceso que tiene un comienzo pero no tiene un final ya que es una actividad de mejora continua que requiere el compromiso y soporte de toda la organización para tener éxito.

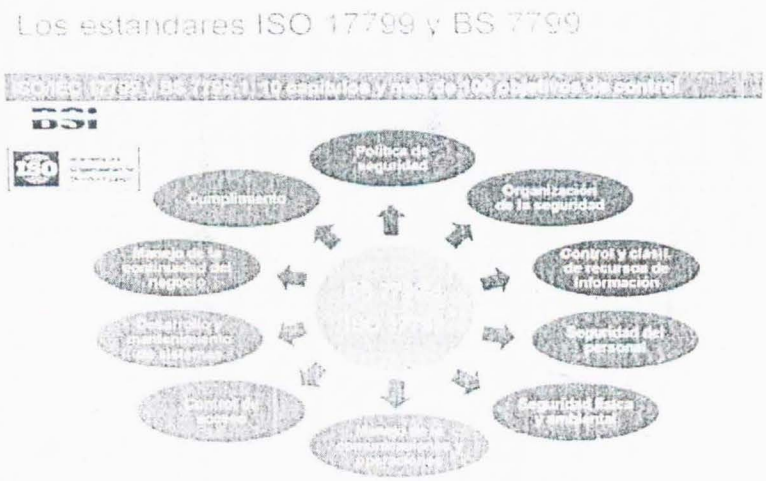
4.4 ESTRATEGIAS PARA LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN EN LAS FUERZAS MILITARES

Como ya se ha mencionado, el cuidado de la información debe ser un proceso permanente y no sólo una acción esporádica, que requiere el compromiso de cada uno de los funcionarios de la Institución Castrense como usuarios finales de los sistemas de información o de la información general de las Fuerzas. Por eso una

[5] Norma ISO 17799:2005

de las tareas más importantes para las FFMM, como parte de la estrategia de seguridad, es crear hábitos en el personal dirigidos al cuidado de la información ya sea confidencial o no, toda vez que está ligada de una manera u otra con la defensa y seguridad del País.

Figura 1. Esquema de la Norma



Para esto es fundamental desarrollar una estrategia de concienciación en seguridad (Conocimiento de la Seguridad, llamado como "Security Awareness" en el medio informático), que involucre actividades que tengan como objetivo garantizar que todos los funcionarios públicos de las FF.MM. interioricen la importancia de proteger la información y utilicen las mejores prácticas para su cuidado. Los principales conceptos y tópicos que se recomiendan para lograr buenos resultados ó el éxito son:

- Inculcar en el conciente y subconsciente de los funcionarios la importancia de cuidar y proteger toda la información en todos los niveles.

- Aumentar el nivel de seguridad de la información en el Comando General y las Fuerzas, minimizando los incidentes que se puedan presentar por falta de conocimiento o malas prácticas del personal.

- Familiarizar a todos los usuarios con los conceptos necesarios relacionados con seguridad de la información.

Para desarrollar un programa eficiente de Concienciación de la Seguridad de la Información se requiere un gran esfuerzo en el nivel de educación interna, donde todos los empleados en sus diferentes roles comprendan la importancia de proteger la información y se vean involucrados en un ambiente donde la seguridad forme parte de los valores y por ende de la cultura del medio militar.

El proceso debe ser impulsado por el Comando General y Comandantes de Fuerza y liderado por los Jefes de las Inspecciones, Jefaturas de Inteligencia (Sección de Contrainteligencia), Oficinas de Recursos Humanos, Control Interno y especialmente por los líderes del área de Tecnología de Información. Además, por medio de estos últimos se debe desplegar y multiplicar, así como promover el aprendizaje individual de manera eficiente, ordenada y didáctica, basados en los diferentes perfiles presentes en el personal directivo, relacionado con tecnología y usuarios en general.

Los aspectos que no pueden estar ausentes en el plan son: riesgos y oportunidades en seguridad de la información, ahorro de costos económicos gracias a una buena política de seguridad, definición de una estrategia de seguridad y aspectos jurídicos de seguridad de la información. Como toda estrategia que busque la interiorización y cambio de cultura, lo fundamental para que sea realmente exitosa es la planificación como un proceso continuo.

Como los problemas de seguridad informática día a día tienen un mayor impacto

sea cual sea su ambiente tecnológico, estos pueden ser provocados por robo de identidad, problemas internos, por diferencias personales, por descuido ó por códigos maliciosos, entre otros; hoy en día estos inconvenientes hace que los proyectos, estrategias y políticas en seguridad informática cobren mayor importancia en las Fuerzas Militares o en cualquier organización particular, no interesando si se requiere inversión presupuestal para minimizar estos riesgos; lo vital es, lograr la reducción de este tipo de incidentes por medio de estrategias que le permitan a la institución orientar de manera inteligente y acertada el gasto.

Las estrategias de seguridad deben ser sostenibles, duraderas e inteligentes, basadas en soluciones o actividades específicas de acuerdo con las necesidades técnicas reales y a la lógica de la Organización Militar que permitan mantener un adecuado control y administración del riesgo.

4.5 LA IMPORTANCIA DE LA HISTORIA Y ESTADÍSTICA EN LA DEFINICIÓN DE LAS POLÍTICAS Y ESTRATEGIAS DE SEGURIDAD INFORMÁTICA

Para el Oficial de Seguridad de la Información, la Oficina de Tecnologías de la Información y la Sección de Contrainteligencia es muy útil contar con un estudio detallado de cada uno de los incidentes por falta de seguridad en el manejo de la información, las horas que el personal trabajó en ellos, el tiempo transcurrido desde que se identificó el evento hasta que se logró la resolución del mismo, los impactos que tuvo el incidente ante las áreas usuarias, ante los clientes de la información, ante otro tipo de organizaciones (especialmente de control y fiscalización, proveedores, etc.) para desarrollar, sustentar y vender las estrategias y políticas de seguridad informática, así como para cuantificar los costos y el tipo de impacto (daños, pérdidas, imagen, etc.) en la Institución ante los altos mandos y demás personal, de tal forma, que se resalte la importancia de la seguridad de la

información en desarrollo del trabajo diario y logro de los objetivos constitucionales.

El desarrollo y la implementación de estrategias para fortalecer y crear cultura de seguridad de la información requiere de recursos presupuestales; siempre es mejor tener un costo o estadística, aunque sea inexacto, de los incidentes por la falta de seguridad informática; especialmente cuando lo que se necesita es justificar inversiones y recursos humanos. Si el oficial de seguridad logra hacer un compromiso en reducir esos costos en un porcentaje que sea atractivo, seguramente logrará obtener el presupuesto que requiere. Igualmente esto afectará el cumplimiento de los objetivos y posicionamiento del área de seguridad informática en las Fuerzas Militares.

4.6 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS

Todas las actividades relativas a la seguridad de una base de datos deben estar guiadas por una arquitectura y estrategia generadas específicamente para cubrir esta necesidad como un componente clave e indispensable de la seguridad de la Institución. La arquitectura debe descansar en una administración estricta de la información y su medición debe estar documentada y embebida en la misma base de datos a través del diseño, implantación, actividades de gestión y continuo monitoreo.

"La seguridad de la información no es un producto – es una combinación de procesos, procedimientos y productos que en conjunto protegen los activos de información y refuerzan los objetivos de negocio".[6]

Los ingredientes fundamentales en la formación de una completa estrategia para la seguridad de la información de las bases de datos alineada con los objetivos de las Fuerzas deben incluir:

- **Dirección** mediante políticas, estándares y procedimientos para el diseño de las bases de datos, su clasificación y configuraciones de seguridad

- **Arquitectura** de las bases de datos existentes para incluir inventario y clasificación de tipos de datos, así como la utilización de metadatos para 'marcar' información sensible o regulada en nuevos diseños

- **Administración** para asegurar que solo los usuarios autorizados tienen acceso directo a sus bases de datos y pueden desempeñar solamente las funciones necesarias para su trabajo

- **Cambios de Administración** para asegurar que los cambios en los esquemas de la base de datos, tablas y columnas, actualización y parches son autorizados apropiadamente y probados antes de ser implantados

- **Controles Técnicos de Seguridad** para asegurar que las configuraciones de seguridad de la base de datos tales como cuentas de usuarios, claves de acceso y controles de acceso son configurados adecuadamente

[6] http://www.embarcadero.com/news/press_releases_latinamerica/Seguridaddatos-sp.html 14-mar-07

- **Auditoría** para proveer un historial detallado de toda la actividad dentro de la base de datos para investigaciones y cumplir con las regulaciones de privacidad relativas al rastreo de quién ha tenido acceso a la Información de Identificación Personal de algún usuario.

La visión y administración estratégica de la información encierra prácticas esenciales que permite a las Instituciones mejorar la disponibilidad, integridad, accesibilidad y seguridad de los activos de información. Permite a su vez, convertir los datos corporativos en información que realmente apalanca las actividades del Sector Defensa llevándole a una mayor capacidad de crecimiento y competitividad.

La seguridad de la información en las Fuerzas Militares se vuelve crítica cuando pensamos en las posibilidades de acceso directo e indirecto a los datos por los usuarios, organismos de control, proveedores, ciudadanía, grupos armados ilegales; sin poder determinar de manera precisa si el uso y manejo es el correcto, ,por lo que "Salvaguardar y rastrear cada movimiento de la información" es una misión crítica; por esta razón, se deben diseñar estrategias que permitan a las empresas desarrollar las mejores prácticas para la administración efectiva de la información, en las cuales se deben considerar las siguientes recomendaciones:

4.6.1 "Principales consejos de seguridad."[7] A continuación se describen algunos consejos para considerar en la formulación de estrategias y políticas de seguridad informática:

- Crear sus políticas de seguridad sobre la base de estándares de la industria mundiales.

- Implementar una defensa de múltiples niveles, con múltiples proveedores.

[7] http://www.sun.com/emrkt/innercircle/newsletter/latam/1206latam_sponsor.html 14-mar-07

- Utilizar los mejores asociados de seguridad en su clase, para ayudar a reducir los costos, mejorar la flexibilidad y permitir que la seguridad organizacional sea más escalable

- Garantizar que todas las políticas de seguridad tengan un enfoque en el cual la complejidad del sistema no se reduce a la suma de sus elementos, sino que constituye un sistema global integrado regido por leyes y normas, que involucra a los profesionales de Tecnologías de la Información, el personal de seguridad física, los equipos de control interno y Secciones de Contrainteligencia, así como a los usuarios mismos.

- Asegurarse de que los funcionarios entiendan que ellos son los principales actores en una política de seguridad exitosa

4.7 LAS ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ACTUALIDAD, CON UN MUNDO GLOBALIZADO

Algunas de las estrategias en las que pueden confiar las empresas para mantener la información protegida y segura, se contemplan en las siguientes consideraciones:

La diferencia entre el pasado y el presente, es que hoy en día las áreas y los profesionales de seguridad tratan de proteger empresas globales y economías internacionales por el fenómeno de globalización. Las Organizaciones deben proporcionar acceso seguro a la información, en cualquier dispositivo, en cualquier lugar y a cualquier hora. La complejidad de las amenazas evoluciona siempre; sin embargo, en general, el volumen de la matriz de la amenaza cambia desde las intrusiones clásicas como el correo basura (spam), hasta los esquemas muy

elaborados por parte de personas que hacen un estudio sofisticado para conseguir los puntos débiles en la seguridad de una empresa y violarlos.

Tradicionalmente, los esfuerzos de seguridad se han concentrado en la protección de la periferia (mediante el uso de firewalls) de las Instituciones, para mantener alejados a los chicos malos, pero aparte del comportamiento malicioso, la forma de trabajar en la actualidad, avances tecnológicos, la masificación del uso del computador y diversidad de usos legales, comerciales, etc. contribuyen con la creciente complejidad del reto de seguridad. Por lo que es necesario trabajar en coordinación con la administración de riesgos, disponer de un robusto y amplio plan de recuperación de desastres, a fin de reducir cualquier riesgo para las operaciones de las Fuerzas Militares, en caso de un siniestro por manos enemigas, descuido o catástrofe natural.

Otra estrategia recomendada para cualquier organización es tener profesionales de seguridad experimentados. Que ellos sean el elemento fundamental y motivador del equipo de seguridad. Hay que mantenerlos capacitados y en entrenamiento permanente.

Establecer e implementar sólidas políticas de seguridad. Todas las empresas necesitan un conjunto sólido de políticas. Estas políticas rigen la forma en la cual una empresa implementa una estrategia de seguridad y los procedimientos operativos alrededor de esa estrategia que se ponen en funcionamiento. Además, es necesario crear las políticas sobre la base de los mejores estándares de la industria en su género. Una vez que la empresa tiene una política de seguridad, debe implementarla y esa implementación debe ser controlada, utilizando esos estándares de la industria. Esto es particularmente importante al momento de hacer una auditoria o control interno. Durante una auditoria, el auditor primeramente preguntará si hay una política en funcionamiento y si se está implementando. La siguiente pregunta será si se ha adoptado un estándar

industrial. Si la respuesta a esas preguntas es "sí", significa que se ha avanzado y se está en una mejor posición para reducir los riesgos informáticos.

Otra importante herramienta es la implementación de una defensa de múltiples niveles o anillos de seguridad, lo cual es más difícil penetrar. De igual forma, la defensa necesita ser no sólo de múltiples niveles sino también de múltiples proveedores para el caso de tecnologías de diferentes marcas. Si alguien penetra un nivel, es más difícil quebrantar los otros niveles, en particular, si se basan en tecnologías de diferentes casas fabricantes.

Se deben establecer estrategias tendientes a filtrar mensajes de correo basura y virus diariamente tanto en las redes, como en las puertas de enlace para evitar que los virus se extiendan. Igualmente, se debe involucrar al equipo de administración o certificación si existe, para que ayuden a supervisar las redes 24 horas al día, los 7 días de la semana. Cuando se produzca un incidente, se debe informar inmediatamente a la dirección y se debe tomar acción. Además, es importante tener sensores de intrusiones en la red, de modo que si alguien trata de penetrar las redes, el equipo humano debe controlar la situación inmediatamente. Se debe estar muy alerta cuando se trata de proteger el perímetro de las redes.

Otro factor que se debe considerar en la generación de las estrategias desde una perspectiva de seguridad, es que hoy en día se lidia constantemente con la proliferación de dispositivos (equipos electrónicos como celulares, memorias, agendas, ipod, etc). Existen muchos dispositivos nuevos portátiles e inalámbricos y todos ellos se conectan a la red y pueden acceder los datos de la Institución. Las Fuerzas deben prestar especial atención a todos estos dispositivos, manejarlos cuidadosamente, poner defensas en funcionamiento y educar a los empleados con respecto a su debido uso.

Es importante establecer una estrategia y procedimiento para cuando se pierde información personal o incluso si sospecha que ha habido una violación de privacidad de la información, por ejemplo se reglamentar, comunicar y ejecutar sanciones significativas.

En resumen todas las organizaciones no importa su tamaño, actividad o sector deben implementar un sólido conjunto de políticas y estrategias de seguridad, basar el sistema gerencial de seguridad en la implementación de estándares de la industria y alinearlo con los objetivos de las Fuerzas o negocio. Si una empresa no tiene mucho dinero y recursos, o aún si los tuviera, una de las acciones más efectivas que pueden tomar las organizaciones es tener un programa de concienciación de seguridad, como parte del sistema gerencial de seguridad. Éste es claramente un programa beneficioso y rentable.

Todos los empleados de cualquier organización deben pensar en seguridad todo el tiempo, más aún cuando se trata de entidades cuya misión es la defensa y soberanía nacional del estado y de sus Instituciones. La concienciación de la seguridad informática reduce costos. Ayuda a proteger a los mismos empleados, compatriotas y logro de los objetivos institucionales.

Si se quieren minimizar los riesgos en los procesos de información, la implementación de un sistema gerencial de seguridad completo en toda la organización es clave para el éxito de las políticas de seguridad.

4.8 ALGUNAS ESTRATEGIAS DE SEGURIDAD INFORMÁTICA PARA LAS FF.MM.

A continuación se describen y recomiendan algunas estrategias para las FF.MM. producto de la experiencia de los autores de este documento, las cuales se pueden complementar con el análisis de las estadísticas, antecedentes y registros de los incidentes y problemas por la falta de seguridad de la información que tengan documentados las Direcciones de Tecnologías de información, Departamentos de Telemática y Secciones de Contrainteligencia de cada Fuerza.

La primera es desarrollar una campaña agresiva para crear cultura personal de la seguridad de la información. Cuando se habla de información, su riesgo y su seguridad, siempre se debe considerar el factor humano, ya que podría definir la existencia o no de los más altos grados de riesgo. Por lo cual es muy importante considerar la idiosincrasia del personal de la Institución basados o guiados en:

- Desarrollar en la Institución el proceso de: "planear, organizar coordinar dirigir y controlar las actividades relacionadas con mantener y garantizar la integridad física de los recursos implicados en la función informática así como el resguardo de los demás activos de las FF.MM.

- Sensibilizar al personal directivo o alto mando de la Institución en torno al tema de seguridad informática.

- Previamente, realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.

- Establecer un sistema integral de seguridad informática que contemple:

    - Definir elementos administrativos del sistema

- Definir políticas de seguridad a nivel Institucional y por áreas
- Organizar y dividir las responsabilidades
- Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- Definir prácticas de seguridad para el personal
- Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extinguidores).
- Números telefónicos de emergencia
- Definir el tipo de pólizas de seguros
- Definir elementos técnicos de procedimientos
- Definir las necesidades de sistemas de seguridad para hardware, software, flujo de energía, cableados locales y externos
- Aplicación de los sistemas de seguridad incluyendo datos y archivos
- Planificación de los papeles de los auditores internos y externos
- Planificación de programas de desastre y sus pruebas (simulación)
- Planificación de equipos de contingencia con carácter periódico
- Control de desechos de los nodos importantes del sistema
- Política de destrucción de basura, copias, fotocopias, etc.
- Consideración de las normas ISO o demás estándares para la seguridad informática

- Desarrollar un proceso que responda a las aristas del triángulo de la figura 2, donde se resalta la tecnología de la información y las comunicaciones TIC como facilitador o componente central para hacer diferenciación y el marketing interno, una empresa no vende hacia fuera lo que no vende adentro, de ahí la importancia del "Modelo de interiorización de deberes en

seguridad de la información, para convertirlos en hábitos", en una empresa que vende seguridad y confianza como es las Fuerzas Militares de un país.

FIGURA 2. RETOS DEL MERCADO DE SERVICIOS

- Elaborar un plan para un programa de seguridad integral, que contemple entre otras las siguientes características:

  - El plan de seguridad debe asegurar la integridad y exactitud de los datos.
  - Debe permitir identificar la información que es confidencial.
  - Debe contemplar las áreas de uso exclusivo.
  - Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles.

- Debe asegurar la capacidad de la organización para sobrevivir a accidentes.
- Debe proteger a los empleados contra tentaciones o sospechas innecesarias.
- Debe contemplar la administración contra acusaciones por imprudencia

- Establecer indicadores para medir el estado y avance de la seguridad informática de la Institución, uno de ellos como punto de partida para conocer la seguridad puede ser:

  Seguridad = riesgo/medidas preventivas y correctivas

  Donde el **Riesgo** puede ser: roles, fraudes, accidentes, terremotos, incendios, etc. y las **Medidas Preventivas y Correctivas** podrían ser: políticas, sistemas de seguridad, planes de emergencia, plan de respaldo, seguridad de personal, etc

- A nivel de personal. Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una concienciación para obtener una autoevaluación de su comportamiento con respecto al sistema, que lleve a la persona a: asumir riesgos, cumplir promesas e innovar.

  - Motivar. Se deben desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel institucional, de cargo e individual.

  - Capacitación General. En un principio, al alto mando con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este

punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo.

- Desarrollar las prácticas sobre la implantación y ejecución de planes de contingencia y la simulación de posibles delitos.

- Capacitación de Técnicos o personal especializado en seguridad informática, encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para transmitir el conocimiento a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

- Ética y Cultura. Se debe establecer un método de educación estimulando el desarrollo y crecimiento de elevados principios morales, que tengan repercusión a nivel personal e institucional. De ser posible realizar conferencias periódicas sobre: doctrina, seguridad, nuevos peligros, accidentes ocurridos.

- ¿Cuándo se logra la seguridad en la organización? Cuando la seguridad es inconciente, cuando hace parte del inconciente de las personas; cuando a través de programas de entrenamiento, se hace tan repetitiva que queda en el inconciente colectivo, convertida en hábitos, en algo cotidiano.
- Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

- Introducir el tema de seguridad informática en la visión de la institución.

- Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.

- Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.

- Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.

- Elaborar ó revisar y fortalecer si existen, los reglamentos y directivas sobre seguridad informática en la Institución.

- Vender todo el esquema y cultura de seguridad informática al alto mando con la idea "Los beneficios de un sistema bien elaborado de cultura de seguridad informática son inmediatos, ya que la institución trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos: aumento de la productividad y motivación del personal, compromiso con la misión de las FF.MM., mejora de las relaciones en el clima laboral y ayuda a formar equipos competentes.

- Desarrollar una campaña publicitaria con folletos, afiches, correos, carteleras, videos, propaganda, etc., con el contenido de los aspectos mencionados anteriormente.

- Establecer responsables de la seguridad informática en la Institución a través de un Comité interdisciplinario.

- Destinar recursos presupuestales para el desarrollo de los cursos de seguridad, elaboración de las ayudas de audiovisuales, campañas, concursos, premios, etc

- Registrar y llevar un control detallado de todos los eventos ocurridos que atentan o afectan la seguridad informática, para posteriormente generar estadística de los mismos y un análisis con el fin de fortalecer dichas áreas.

5. POLÍTICAS EN LA SEGURIDAD DE LA INFORMACIÓN

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las Fuerzas Militares hoy día en lo que se refiere a la protección de la información frente a peligros externos e internos.

Las políticas de seguridad informática son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base del plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

Las políticas incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación con las violaciones de seguridad. A menudo estas políticas se pueden acompañar de normas, instrucciones y procedimientos.

Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. Por otro lado, las políticas son de jerarquía superior a las normas, estándares y procedimientos que también requieren ser acatados. Las políticas consisten en declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos en detalle.

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos y los procedimientos. Por ejemplo, una norma de seguridad de cifrado podría especificar el uso del estándar DES (Data Encryption Standard). Esta norma probablemente deberá ser revisada o reemplazada en los próximos años.

Una declaración sobre políticas describe sólo la forma general de manejar un problema específico, pero no debe ser demasiado detallada o extensa, en cuyo caso se convertiría en un procedimiento.

Las políticas también son diferentes de las medidas de seguridad o de los mecanismos de control. Un ejemplo de esto último sería un sistema de cifrado para las comunicaciones o para los datos confidenciales guardados en discos y cintas. En muchos casos las políticas definen metas u objetivos generales que luego se alcanzan por medio de medidas de seguridad.

En general, las políticas definen las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad. Las políticas podrían dictar que todo el software desarrollado o adquirido se pruebe a fondo antes de utilizarse. Se necesitará tomar en cuenta varios detalles sobre cómo aplicar esta política. Por ejemplo, la metodología a usar para probar el software.

Un documento sobre políticas de seguridad contiene, entre muchos aspectos: definición de seguridad para los activos de información, responsabilidades, planes de contingencia, gestión de contraseñas, sistema de control de acceso, respaldo de datos, manejo de virus e intrusos. También puede incluir la forma de comprobar el cumplimiento y las eventuales medidas disciplinarias.

5.1 ¿POR QUÉ SON IMPORTANTES LAS POLÍTICAS?

5.1.1 Porque aseguran la aplicación correcta de las medidas de seguridad.

Las Fuerzas Militares necesitan de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad.

5.1.2 Porque guían el proceso de selección e implantación de los productos de seguridad. La mayoría de las organizaciones no tienen los recursos para diseñar e implantar medidas de control desde cero. Por tal razón, a menudo se escogen soluciones proporcionadas por los fabricantes de productos de seguridad y luego intentan adaptar esos productos a las políticas, procedimientos, normas y demás esfuerzos de integración dentro de la Entidad. Esto se realiza a menudo sin conocer o entender suficientemente los objetivos y las metas de seguridad. Como resultado, los productos de seguridad escogidos y su aplicación pueden no resultar adecuados a las verdaderas necesidades de la organización.

Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía el alto mando y los funcionarios de las Oficinas de Telemática y Secciones de Contrainteligencia, en lo que a seguridad se refiere. De manera que tales políticas pueden ser una forma de garantizar que se están seleccionando, desarrollando e implantando los sistemas de seguridad, apropiadamente.

5.1.3 Porque demuestran el apoyo del alto mando. La mayoría de las personas no están conscientes de la gravedad de los riesgos relativos a la seguridad y por eso no se toma el tiempo para analizar estos riesgos a fondo. Además, como no tienen la experticia suficiente, no son capaz de evaluar la necesidad de ciertas medidas de seguridad. Las políticas son una manera clara y definitiva para que la alta dirección pueda mostrar que:

a. La seguridad de los activos de información es importante.
b. El personal debe prestar la atención debida a la seguridad.

5.1.4 Para evitar problemas legales. Se presentan cada vez más casos judiciales en los cuales se encuentra responsables a empleados, y particularmente a jefes/directores, de no actuar apropiadamente bien en lo referente a seguridad informática. La razón puede ser atribuida a: negligencia, violación de confianza, fallas en el uso de medidas de seguridad, mal práctica, etc. Estos casos se pueden usar con éxito para llamar la atención del alto mando y para lograr apoyo para los esfuerzos en seguridad informática.

5.1.5 Para lograr una mejor seguridad. Uno de los problemas más importantes en el campo de seguridad informática lo representan los esfuerzos fragmentados e incoherentes. A menudo una dependencia estará a favor de las medidas de seguridad, mientras que otra dentro de la misma organización se opondrá o será indiferente. Si ambas dependencias comparten recursos informáticos (por ejemplo una LAN o un servidor), la Oficina que se opone pondrá en riesgo la seguridad de la otra dependencia y de la Institución completa. Aunque no es ni factible ni deseable que todas las personas en una organización se familiaricen con las complejidades de la seguridad informática, es importante que todas ellas se comprometan con mantener algún nivel mínimo de protección. Las políticas pueden usarse para definir el nivel de esta protección mínima, a veces llamada línea de base.

5.2 POLÍTICAS Y PROCEDIMIENTOS EN SEGURIDAD DE INFORMACIÓN

Antes de embarcarse en un esfuerzo de promulgar y aplicar las políticas de seguridad, es aconsejable aclarar quién es responsable de esta actividad. Si se ignora este aspecto importante, se corre el riesgo de posteriores objeciones, críticas y malentendidos, que pueden significar problemas y grandes retrasos.

Otro requisito previo necesario para tener éxito involucra al alto mando. Sólo después de que sus miembros tomen conciencia de que los activos de información son un factor vital para el éxito de la Institución, es que la seguridad informática es apreciada como un asunto serio que merece atención. En caso contrario, probablemente no apoyen la idea de establecer políticas de seguridad.

El alto mando debe darse cuenta que hay problemas serios de seguridad y que se requiere de políticas para afrontarlos. El trabajo previo incluye a menudo una breve presentación al personal directivo para sensibilizarlo sobre la necesidad de la seguridad informática.

Idealmente, el desarrollo de políticas de seguridad debe comenzarse después de una evaluación a fondo de las vulnerabilidades, amenazas y riesgos. Esta evaluación debería indicar, quizás sólo a grandes rasgos, el valor de la información en cuestión, los riesgos a los cuales esa información se sujeta y las vulnerabilidades asociadas a la manera actual de manejar la información.

Las políticas pueden publicarse en material tal como video, carteles o artículos en revistas y boletines. Las políticas deben revisarse en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas.

5.2.1 ¿Cómo deben elaborarse las políticas?

a) Recopilar material de apoyo. Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgos que indique claramente las necesidades de seguridad actuales de la organización. Antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención.

Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de la Institución (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

b) Definir un marco de referencia. Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir políticas que se piensan aplicar de inmediato así como aquellas que se piensan aplicar en el futuro.

c) Redactar la documentación. Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, entonces se estará listo para redactar las políticas, para lo cual puede servir de ayuda el ejemplo que se encuentra más adelante.

Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia. Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podrá recibir un documento considerablemente más largo que proporciona mucho más detalles.

d) Revisión. Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración del Alto Mando para su aprobación. Este comité debería tener representantes de las distintos dependencias de la organización y una de sus funciones más importantes es evaluar las políticas en la luz de su viabilidad, análisis costo/beneficio y sus implicaciones. Las preguntas que debe contestar son, por ejemplo: ¿Son

estas políticas prácticas y fácilmente aplicables?. ¿Son estas políticas claras?

e) Aprobación personal directivo. Es muy importante que el Alto Mando apruebe las políticas, teniendo en cuenta el caso frecuente en que ciertos funcionarios objetan o piensan que ellos no necesitan obedecer.

Además, es fundamental que luego de la entrada en vigor, las políticas se apliquen estrictamente, ya que de otra forma se puede fomentar la hipocresía entre los empleados y la tolerancia por conductas inapropiadas. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto.

La aplicación de nuevas políticas es a menudo más eficaz si el personal ha sido informado de exactamente qué actividades representan trasgresiones de la seguridad y qué penalización recibirían si fueran encontrados culpables.

Un curso o taller de sensibilización es una forma muy efectiva para dar a conocer las nuevas políticas. Allí, por ejemplo, se explicaría que la información interna es propiedad de la organización, y que no puede ser copiada, modificada, anulada o usada para otros propósitos sin la aprobación del superior inmediato o dueño de la información.

La extensión y el grado de detalle de las políticas están en función del tipo de audiencia y pueden haber distintos documentos según el caso. Por ejemplo, podría haber documentos para los usuarios, la gerencia y el personal de informática. Muchas de las políticas en cada uno de estos documentos serían iguales, aunque el grado de detalle, las palabras técnicas utilizadas, y el número de ejemplos puede variar de un documento a otro. Para los usuarios finales, el documento debe limitarse a unas cuantas páginas. Para la gerencia habrá consideraciones adicionales, tal como los aspectos legales, y es probable que esto extienda el documento. Para el personal técnico será todavía más largo y más

detallado.

Otro factor que afecta es el grado de seguridad requerido en la organización. En general, cuánto mayor es el uso de la información para las actividades de una organización, mayor es la necesidad de seguridad. Por supuesto que actividades especialmente delicadas, tal como salud y defensa, requieren de políticas muy detalladas.

Adicionalmente al número de políticas, hay que plantearse cuán larga debe ser la definición de cada política. Las definiciones concisas, de unas cuantas frases, son más aceptadas por los empleados ya que son más fácilmente leídas y entendidas. En todo caso deben ser suficientemente especificas para ser entendidas e interpretadas sin ambigüedad, pero no deben ser tan específicas que impidan adaptarlas a las condiciones particulares de un sitio o departamento.

Se aconseja elaborar un primer conjunto de políticas corto y relativamente fácil de cumplir por parte del personal. Después, cuando haya sido implantado y asimilado a lo largo de la Institución, se puede preparar una lista más completa y más estricta. Es mejor proceder de forma relativamente lenta, con una serie de pasos en el desarrollo de políticas, y así lograr credibilidad y apoyo, en lugar de preparar de una vez un solo documento extenso con todas las políticas, el cual seria rechazado porque puede ser percibido como engorroso o excesivamente severo.

5.3 ALGUNAS DE POLÍTICAS DE SEGURIDAD

5.3.1 Justificación. Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestras Fuerzas. Sin ellos nos quedaríamos rápidamente fuera del combate e incumpliendo la misión

encomendada, por tal razón el Alto Mando tiene el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén correctamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Institución debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico ó conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas dependencias de las Fuerzas están en el deber y con la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el Comité de Seguridad Informática deberá llevar a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se recomienda preparar cada año un informe para el alto mando que muestre el estado actual de la Institución en cuanto a seguridad informática y los progresos que se han logrado, con referencia al anterior periodo.

A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Institución. Debe

hacerse hincapié en que la seguridad informática es una actividad tan vital para las Fuerzas como lo son las operaciones militares en la defensa y seguridad del país, o los procesos de contabilidad y nómina a nivel administrativo.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Institución (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias.

5.3.2 Políticas para definir responsabilidades. Los siguientes entes son responsables, en distintos grados de la seguridad en las Fuerzas:

- El Comité de Seguridad Informática está compuesto por los representantes de las distintas dependencias de la Institución, así como por el Jefe de Informática, Jefe Comunicaciones (cuando exista) y el Jefe del área jurídica. Este Comité estará encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También será responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones trimestrales o ad hoc, el Comité efectuará la evaluación y revisión de la situación de la Institución en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos que afecten la seguridad.

- Las Direcciones de Informática/Telemática serán responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Sección de Contrainteligencia y las Oficinas

de Control Interno. También será responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas correctivas pertinentes.

- El Administrador de cada sistema informático es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y debe llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo: aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

- Los usuarios son responsables de cumplir con todas las políticas de la Institución Castrense relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

- No divulgar información confidencial de la organización a personas no autorizadas.

- No permitir y no facilitar el uso de los sistemas informáticos de las Fuerzas Militares a personas no autorizadas.

- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono y fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Institución.

- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

- Reportar inmediatamente a su jefe a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de las Fuerzas y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

5.3.3 Políticas de seguridad para computadores.

- Los computadores de la Organización Castrense sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

- Los equipos de la Institución sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

- Debe respetarse y no modificar la configuración de hardware y software establecida por las Direcciones de Informática/Telemática.

- No se permite fumar, comer o beber mientras se está usando un PC.

- Deben protegerse los equipos de riesgos del medio ambiente, por ejemplo, polvo, incendio y agua.

- Deben usarse protectores contra transmisores de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS) cuando no existe corriente regulada.

- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios informáticos.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso. Las medidas que se recomiendan incluyen el uso de puertas, divisiones, cámaras, guayas y cerradura con llave.

- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Institución se requiere una autorización escrita del Jefe de cada dependencia y del Ayudante General de cada Fuerza.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina ó puesto de trabajo.

- Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales/secretos se deben borrar.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir,

modificar, crear o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente al Jefe de la Dependencia y al Oficial de Seguridad.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de las LAN del Ministerio ó de cada Fuerza.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software la Institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón, es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Los usuarios no deben copiar a un medio removible (como un diskette, CD ó USB), el software o los datos residentes en las computadoras de las Fuerzas, sin la aprobación previa de la Oficina de Telemática / Informática.

- No pueden extraerse datos fuera de las sedes de la Institución sin la aprobación previa de Jefe de la Jefatura o Departamento. Esta política es particularmente pertinente para aquellos que usan computadoras portátiles o están conectados a Internet.

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Atención al Usuario / Centro de Cómputo y poner la PC en cuarentena (aislado de la red) hasta que el problema sea resuelto.

- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la Organización Militar.

- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Oficina de Tecnologías de Información / Telemática.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la Oficina de Tecnologías de Información / Telemática.

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- No deben usarse diskettes, USB u otros medios de almacenamiento en cualquier computadora de la Institución a menos que se haya

previamente verificado que están libres de virus u otros agentes dañinos.

- Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores; las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de las Fuerzas deben guardarse en otra sede, lejos del edificio habitual.

- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador del Centro de Cómputo o en su defecto cada uno de los funcionarios de esos sistemas son responsables de hacer copias de respaldo periódicas. Los directores de los distintos departamentos / dependencias / secciones son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

- La información de la Institución clasificada como secreto, confidencial, sensible o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Oficina de Tecnologías de Información o equivalentes.

- No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

- Siempre que sea posible, debe eliminarse información confidencial de de los computadores y unidades de disco duro antes de mandarlos a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la Institución.

- El personal que utiliza un computador portátil que contenga información confidencial de la Institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje. Toda información confidencial y secreta debe estar cifrada.

5.3.4 Políticas de seguridad para las comunicaciones.

- Propiedad de la información. Con el fin de mejorar la productividad, las Fuerzas promueven el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Institución y no propiedad de los usuarios de los servicios de comunicación.

- Uso de los sistemas de comunicación

- Los sistemas de comunicación de la Institución generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de las Fuerzas Militares.

- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Institución y en tal sentido deben usarse las horas no laborables.

- Confidencialidad y privacidad

  - Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outolook, Outlook Express u otros productos previamente aprobados por la Oficina de Tecnologías de Información o equivalente.

  - Los funcionarios de las FF.MM. no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Institución se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para

lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

- Es política de la Institución no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones pueden ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o control. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un funcionario durante el curso de la resolución de un problema.

- De manera consistente con prácticas generalmente aceptadas, la Institución procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

- Reenvío de mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Institución, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial sin la debida aprobación.

- Borrado de mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que

otros puedan acceder a esa información y además se libera espacio en disco.

5.3.5 Políticas de seguridad para redes

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Institución al tener redes de computadoras. Estas políticas se aplican a todos los funcionarios, contratistas, consultores y personal temporal de las Fuerzas.

- Aspectos generales

Es política de la Institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras organizaciones o personas y que le haya sido confiada.

- Modificaciones

Todos los cambios en la central telefónica (PABX), en los servidores y equipos de red de la Institución, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, negación de servicios o acceso inadvertido a información confidencial.

- Cuentas de los usuarios

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

- No debe concederse una cuenta a personas que no sean funcionarios de la Institución a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a los directamente responsables de la administración o de la seguridad de los sistemas informáticos.

- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o la Oficina de Tecnologías de Información determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses (recomendable). El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un funcionario cesa en sus funciones.

- Cuando un empleado es despedido, retirado o renuncia a la Institución, debe desactivarse su cuenta antes de que deje el cargo.

- Contraseñas y el control de acceso

  - El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

- Para el acceso remoto a los recursos informáticos de la Institución, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Si no ha habido ninguna actividad en una terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario se autentique nuevamente mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Institución, pudiendo ser causal de investigaciones y sanciones disciplinarias.

- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

- Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón, deben protegerse para que

nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

- Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo con tarjetas de proximidad).

5.4. SEGURIDAD DEL PERSONAL

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de ingreso, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario desarrollar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de

subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

5.4.1 Objetivos. Los objetivos de esta subdivisión es dar pautas para reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado. Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Institución en el transcurso de sus tareas normales. Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

5.4.2 Alcance. Esta Política se aplica a todo el personal del Organismo Castrense, cualquiera sea su situación, y al personal externo que efectúe tareas dentro del ámbito de la Institución.

5.4.3 Responsabilidad. El responsable del Área de Recursos Humanos o quien defina las funciones de los cargos incluidos en la TOE, deberá incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la

Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información y a los propietarios de la información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la Institución, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal de las Fuerzas Militares es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

5.4.4 Política Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos.

5.4.4.1 Incorporación de la Seguridad en los Puestos de Trabajo. Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo ó cargos.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

5.4.4.2 Control y Política del Personal. Se llevarán a cabo controles de verificación del personal en el momento en que se requiera el puesto o cargo. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto, tenga la Institución.

5.4.4.3 Compromiso de Confidencialidad. Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de incorporación, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Institución. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra dependencia competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- Suscripción inicial del Compromiso por parte de la totalidad del personal.
- Revisión del contenido del Compromiso cada. .(indicar período).
- Método de resuscripción en caso de modificación del texto del Compromiso.

5.4.4.4 Términos y Condiciones de Empleo. Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la Institución y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

5.4.5 Capacitación del Usuario.

5.4.5.1 Formación y Capacitación en Materia de Seguridad de la Información. Todos los empleados de la Institución y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en las Fuerzas Militares, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de las FF.MM. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso

correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada ..... (indicar periodicidad) se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación.

Áreas Responsables del Material de Capacitación

.....

.....

El personal que ingrese a la Institución recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

5.4.6 Respuesta a Incidentes y Anomalías en Materia de Seguridad

5.4.6.1 Comunicación de Incidentes Relativos a la Seguridad. Los incidentes relativos a la seguridad serán comunicados a través del personal del área informática, de atención a los usuarios, o jefe directo tan pronto como sea

posible. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otras dependencias de competencia, el Responsable de Seguridad Informática, comunicará a la Sección de Contrainteligencia y dueño de la Información todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los empleados y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

5.4.6.2 Comunicación de Debilidades en Materia de Seguridad. Los usuarios de servicios de información, al momento de tomar conocimiento directo ó indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

5.4.6.3 Comunicación de Anomalías del Software. Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Alertar inmediatamente al Responsable de Seguridad Informática o Jefe Inmediato.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado y adecuadamente habilitado.

5.4.6.4. Aprendiendo de los Incidentes. Los Administradores del centro de cómputo o personal de atención a usuario final es una unidad de respuesta ante incidentes en redes, que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten a los recursos informáticos de la Institución, es decir, cualquier ataque o intento de penetración a través de sus redes de información.

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes, costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

5.4.6.5. Procesos Disciplinarios. Se seguirá el proceso disciplinario formal contemplado en las normas que rigen al personal de la Administración

Publica, para los empleados que violen la Política, Normas y Procedimientos de Seguridad de las Fuerzas Militares.

5.4.7 Responsabilidades del Usuario. Aunque ya se habían mencionado algunas con anterioridad, en esta sección se complementan y profundizan.

5.4.7.1 Uso de Contraseñas. Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente sirven para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable de la Información, que:

    - Sean fáciles de recordar.
    - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar de acuerdo a lo establecido en "Comunicación de Incidentes Relativos a la Seguridad", cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas.

5.4.7.2 Equipos Desatendidos en Áreas de Usuarios. Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concienciación a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

5.4.7.3. Protección de Datos y Privacidad de la Información Personal. Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La Institución redactará un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la Fuerza.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita de la Sección de Contrainteligencia, Departamento de Informática y del directo responsable o dueño de la información. A través del "Compromiso de Confidencialidad" se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del funcionario. En particular, se deberán tener presente las normas que tenga la Institución, en cuanto a:

- Establecer que los Funcionarios Públicos deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron

asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera.

- Disponer que todos los funcionarios públicos de las FF.MM. deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueran asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.

- Obligar a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.

- Establecer que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada, sensible ó secreta conforme a las disposiciones vigentes, ni la debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.

- Establecer responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.

- *Confidencialidad*: Impedir la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos honestos, de

información secreta y con valor institucional que haya sido objeto de medidas razonables para mantenerla secreta.

- *Código Penal*: Sanciona a aquel que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa, al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos, al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo, cargo u oficio.

5.4.7.4 Recolección de Evidencia. Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos. Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, la Institución garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo

información secreta y con valor institucional que haya sido objeto de medidas razonables para mantenerla secreta.

- *Código Penal*: Sanciona a aquel que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa, al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos, al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo, cargo u oficio.

5.4.7.4 Recolección de Evidencia. Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos. Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, la Institución garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo

se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

- Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una investigación administrativa, por lo tanto se deben tomar todos los cuidados establecidos para la obtención y preservación de la evidencia.

5.4.7.5. Establecer Sanciones Previstas por Incumplimiento. Se debe sancionar administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas convencionales que rigen al personal de la Administración Pública, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, las Leyes de Procedimiento Administrativo y demás normativas específicas aplicables.

Además de las sanciones disciplinarias o administrativas, se puede reglamentar que el funcionario que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial - cuando ocasiona un daño que debe ser indemnizado- y/o en responsabilidad penal -cuando su conducta constituye un

comportamiento considerado delito por el Código Penal y leyes especiales.

6. CULTURA ORGANIZACIONAL

A continuación se mencionaran algunas definiciones o conceptos universales de cultura organizacional; sin embargo más allá de la definición que se tome, los autores coinciden en que cada empresa tiene una cultura que le es particular, que integra valores, símbolos, comportamientos y asunciones que son ampliamente compartidas en la Organización.

- La "Cultura organizacional, se refiere a la relación múltiple entre los valores, creencias y principios fundamentales que constituyen los cimientos del sistema de gestión de una organización, y que se manifiestan a través de los procedimientos y comportamientos de sus miembros. Así pues, una teoría cultural de la efectividad organizacional considera como premisa básica que los valores, las creencias y los significados que fundamentan un sistema social son la fuente primordial de una actividad motivada y coordinada."[8]

- La literatura administrativa ha adoptado de la sociología el concepto de cultura, definiéndola como: "El conjunto de valores, creencias, ideologías, hábitos, costumbres y normas que comparten los individuos en la organización y que surgen de la interrelación social, los cuáles generan los patrones de comportamiento colectivos que establecen una identidad entre sus miembros y los identifica de otra organización"[9]

La cultura cumple varias funciones en el seno de una organización. En primer lugar, cumple la función de definir los límites; es decir, los comportamientos difieren unos de otros. Segundo, trasmite un sentido de identidad a sus miembros. Tercero, facilita la creación de un compromiso personal con algo más amplio que

---

[8] MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003. P.80

[9] Tomado del documento Gestión del talento Humano, Cultura Organizacional. Programa de Formación de Jefes Familia Bolivar. Mayo 2004

los intereses egoístas del individuo. Cuarto, incrementa la estabilidad del sistema social. La cultura es el vínculo social que ayuda a mantener unida a la organización al proporcionar normas adecuadas de los que deben hacer y decir los empleados.

6.1 RELACIÓN DE LA CULTURA CON LA EFECTIVIDAD

"Las investigaciones recientes demuestran que la cultura organizacional tiene estrecha relación con la efectividad de las organizaciones"[10] afirmación que puede soportarse en el hecho de que compartir valores, creencias y símbolos, comprendidos con un sentido común para todos los miembros de la empresa; da mejor capacidad para generar acciones coordinadas y llegar a acuerdos con mayor facilidad. Igualmente la misión corporativa conduce a un rendimiento efectivo, porque proporciona sentido y propósito.

Una explicación más clara de esta relación esta en la síntesis del capítulo 4 del libro Gestión Humana y Planeación[11] que la describe así: "La naturaleza de una determinada cultura es un reflejo de las estrategias originales de los fundadores de una empresa, así como también las cosas que se han aprendido y conservado con el tiempo. Así pues la cultura de una organización se puede ver como un código, una lógica y un sistema de comportamientos y significados estructurados que han soportado la prueba del tiempo y sirven como una guía colectiva para la adaptación y la supervivencia. Esta definición ayuda a explicar por qué las culturas pueden ser: abstractas y místicas y a la vez concretas e inmediatas; imposibles de cambiar y a la vez rápidamente variables; complejas e intrincadas y a la vez cimentadas en valores muy básicos y a veces inaplicables a problemas específicos pero siempre fundamentales para la estrategia y la efectividad de una

[10] MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003, p.80
[11] Ibid p.84

organización. Esta definición también explica porqué la cultura tiene que estudiarse como causa y como efecto."

6.2 LA NECESIDAD DE CONTROL EN TECNOLOGÍA DE LA INFORMACIÓN COMO PARTE DE LA CULTURA ORGANIZACIONAL

Por lo tanto la nueva Cultura Informática de las Fuerzas Militares debe incorporar, como ya se ha mencionado en los capítulos anteriores "la administración efectiva de la información y de la tecnología de información (TI) relacionada", toda vez que es un elemento crítico para el éxito y la supervivencia de la Institución. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información.
- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

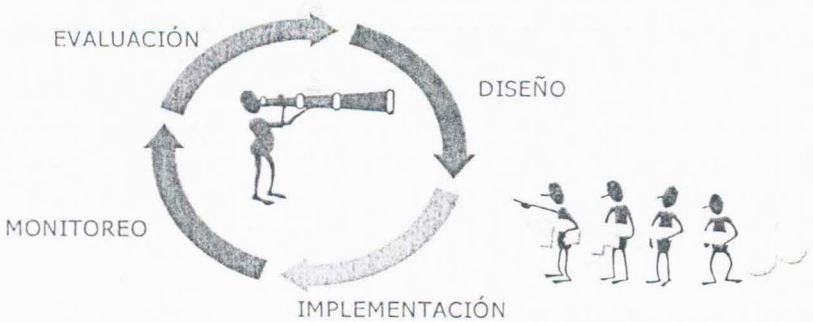
Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor

y equipos Mainframe). Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados"[12], de tal forma que se trasmitan a los usuarios a través de estrategias para interiorizarlos y por ende iniciar el proceso de la concienciación de la seguridad y uso adecuado de la información.

En la figura 3, se observa como los administradores de la información deben establecer los controles para la seguridad de la información, a través de la identificación de riesgos, que se minimizan con políticas y estándares que se definen en el diseño y se implementan a través de prácticas, que si al monitorearlas son inseguras se evalúan nuevamente.

FIGURA 3 CICLO DEL PROCESO DE SEGURIDAD

CICLO DEL PROCESO DE SEGURIDAD



[12]INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION, Comité Directivo de Cobit. Objetivos de Control para la información y Tecnologías Afines. 2ª. Edición. USA, 1998.

6.3 APRENDIZAJE ORGANIZACIONAL

A continuación se describe y siguiere una serie de conceptos que se deben considerar para generar una cultura de la seguridad y uso de la información en las Fuerzas Militares que permiten desarrollar el proceso de aprendizaje organizacional.

6.3.1 El compromiso y la visión personal base para un proceso de aprendizaje significativo. "Todas las organizaciones aprenden. El aprendizaje tiene lugar en todas las empresas, no importa de dónde sean; el mundo cambia y, por lo tanto, la organización también tiene que cambiar. Acá se definen determinadas competencias que las empresas pueden desarrollar para modificar profundamente su capacidad de aprendizaje. Hay muchas formas de comenzar, pero lo importante, para la mayoría de las empresas es que tienen que decidir la importancia que esto tiene para ellas. No hay nada que sustituya al verdadero compromiso y a la visión personal. Es fundamental creer en algo que importe personalmente. Si la gente no se compromete personalmente, no se puede sostener un proceso de aprendizaje significativo. De manera que, de una u otra forma, siempre se comienza por el compromiso13."

---

[13] Tomado de Senge, P. 1998. *Con mucha disciplina.* Santafé de Bogotá: Gestión, Vol. 1, Número 2, enero-febrero, citado por Citado por MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003. P.8-9

Las cinco grandes estrategias que consolidan el aprendizaje organizacional como el fundamento del desarrollo fueron planteadas por Senge en 1995 así:[14]

Conocimiento personal: identificar la capacidad personal que permite lograr los objetivos individuales en armonía con los propósitos de la organización.

Esquemas mentales: acudir a la observación y la reflexión de nuestras actuaciones usuales para identificar la manera como abordamos la realidad y la modelamos de acuerdo con nuestras creencias y paradigmas.

Visión integrada: determinar un lugar común de encuentro con el fin de centrar nuestro esfuerzo y su sentido en el logro de los propósitos que nos convocan, además de definir los lineamientos y principios que se usarán para que la actividad diaria guarde unas mismas reglas del juego para todos.

Aprender en equipo: Despertar en cada uno la importancia del reconocimiento de la diferencia individual como el fundamento de toda integración posible. Adquiere una gran importancia destacar el proceso de comunicación como soporte de la actividad colectiva.

---

[14] Senge, P. 1995. *La Quinta Disciplina.* Barcelona: Granica. Citado por MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003. P.9

Pensar globalmente: El mundo natural no funciona de manera lineal, causa-efecto. La naturaleza es una red infinita de relaciones en las que cada parte adquiere sentido gracias al sentido de la globalidad a la que pertenece. Una empresa, órgano vivo de la vida social, es un agrupamiento de seres humanos que piensan, sienten y actúan con base en las muchas relaciones que establecen en el día a día.

6.3.2 Entrenamiento. "El entrenamiento en las organizaciones es la primera fase de cualquier proceso de capacitación e involucra no solamente un aprendizaje de información para el empleado sino también cambios en la conducta de este que contribuyen al logro de las metas individuales y organizacionales. Es esencial que los procesos de entrenamiento se evalúen teniendo en cuenta su relevancia y pertinencia para el logro de los objetivos organizacionales".15

6.3.3 Formación. 16 La formación es el proceso resultante del conjunto de actividades destinadas a desarrollar en los empleados las habilidades, aptitudes y actitudes que la empresa necesitará en el futuro.

La formación organizacional no tendrá resultados a menos que esté vinculada con los objetivos de la empresa. Un programa de formación bien diseñado surge de los objetivos estratégicos de la compañía. Un programa mal diseñado será aquel que no tenga relación alguna con estos objetivos.

---

[15] MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003. P.10

[16] Ibid, tomado del capítulo 1, sinopsis de los procesos de administración de personal

O lo que es peor, que no los entienda correctamente. Existen varios tipos de formación:

Formación en Habilidades. Es el más habitual en todas las empresas. El panorama es sencillo; la necesidad o deficiencia se identifica mediante un detallado estudio; se generan los objetivos concretos y se crea su contenido para alcanzar esos objetivos. Los criterios para valorar la eficacia de la formación se basarán igualmente en los objetivos que se hayan establecido en la fase anterior.

Formación de actualización. La actualización, un tipo de formación en habilidades, se centra en desarrollar en los empleados las habilidades que requieren para mantenerse al día de las exigencias cambiantes de sus puestos de trabajo.

Formación Interdisciplinaria. Consiste en formar a los empleados para que puedan utilizar sus capacidades en áreas diferentes a los puestos de trabajo asignados o la profesión.

Formación para trabajar en equipo. Cada vez mas las empresas organizan su trabajo en torno a equipos humanos. Algunos hallazgos iniciales pueden utilizarse para guiar las actividades de formación.

Formación en Creatividad. Las empresas buscan caminos para hacer más con menos, y para mantenerse competitivos en un mercado cada vez más poblado. Como un medio para explotar el potencial innovador de los trabajadores, muchas empresas están utilizando la formación en creatividad.

6.4 EL PLAN DE CONCIENCIACIÓN DE LA SEGURIDAD Y CORRECTO USO DE LA INFORMACIÓN

Dentro de la arquitectura de la seguridad el componente de toma de conciencia asegura que los empleados comprendan y aprecien la necesidad comercial de las reglas y procedimientos de seguridad. Tal como se describe en la figura 4 donde se ve que la concienciación hace parte integral de toda la estrategia corporativa.

El objetivo principal del proceso de Concienciación en la Seguridad de la Información es el crear una cultura organizacional en el manejo de la información, adecuada a los requerimientos de las Fuerzas Militares.

FIGURA 4. ESTRATEGIA DE SEGURIDAD CORPORATIVA

Una vez que este operando el área de Seguridad de la Información, se inicia el diseño del proceso de Concienciación para promover la seguridad de la información dentro de los funcionarios de las Fuerzas Militares, a través de la elaboración del ***Programa de Concienciación de la Protección de Información (PCPI)***, definiéndole los siguientes dos objetivos principales: Asegurar que cada empleado o área de las FF.MM. que aplique las Políticas y Estándares de Seguridad. Asegurar que cada funcionario de las FF.MM. entienda su rol y responsabilidad en la protección de la información.

A menudo los usuarios y las personas encargadas de desarrollar el sistema, ven a las políticas, procedimientos y mecanismos de seguridad como barreras que frenan la liberación de las aplicaciones sin considerar que la incorporación de las medidas de protección es parte integral de éstas. Para

ello se propone el modelo de interiorización de deberes en seguridad de la información, convirtiéndolos en hábitos.

6.5 CONCEPTOS BÁSICOS PARA EL ENTENDIMIENTO DEL PROCESO DE APRENDIZAJE DEL INDIVIDUO Y LA ORGANIZACIÓN EN UN CONTEXTO DE GESTIÓN HUMANA ORIENTADA AL MANEJO SEGURO DE LA INFORMACIÓN

Teniendo en cuenta que lo que se pretende rescatar con este estudio es la idea y el concepto que cada uno se forma de aspectos y procesos de negocio, en este caso relacionados con Seguridad de la Información, su importancia, el rol y la responsabilidad de cada uno.

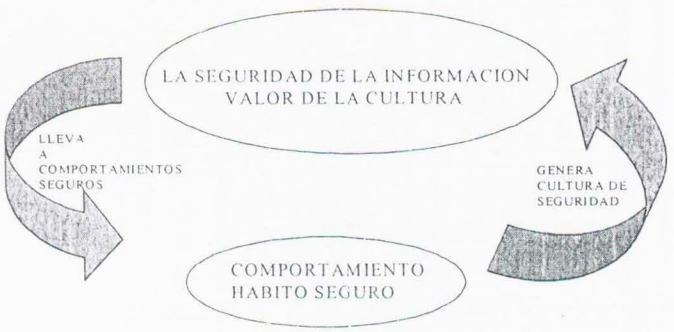
6.5.1 La Cultura Absorbe.

A menudo se pregunta porque la gente cambia su comportamiento cuando llega a ciertas culturas; un caso podría ser ¿por qué cuando se llega a Estados Unidos, se pueden respetar las señales de transito y se admira el respeto por el peatón; y cuando se esta en Colombia en no? La respuesta esta en la misma cultura, la cultura absorbe; pero a su vez esta compuesta por el conjunto de costumbres y hábitos, cumpliendo un ciclo de retroalimentación como el que se muestra en la figura 5.

Si la seguridad de la información es cultura, conformada por un conjunto de costumbres y hábitos que la identifican, esta absorberá rápidamente a los miembros que la componen, pero a su vez si la comunidad tiene hábitos seguros en el manejo de la información conformará una cultura de seguridad

de la información. Esta conclusión explica porque la cultura tiene que estudiarse como causa y como efecto.

FIGURA 5. LA CULTURA ABSORBE



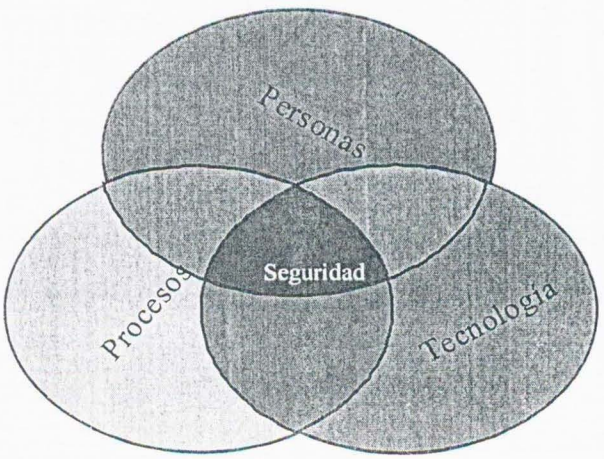
6.5.2 Contexto Relacional de la Seguridad de la Información. La seguridad de la información es una propiedad emergente de las relaciones de tecnología, de los procesos administrativos involucrados y la parte humana, y es así como la Seguridad de la Información es un ente dinámico que se nutre de las relaciones existentes entre estos tres elementos. Como lo muestra la figura 6.

Esta figura ha sido construida a partir de conceptos de diferentes conferencias y jornadas de seguridad de la información en el ambiente tecnológico, hoy es un símbolo en el Comité de Seguridad Informática de muchas organizaciones.

Esta reflexión se hizo a partir de los principios de la complejidad que llevaron a la conclusión de que la seguridad de la información es un sistema complejo

adaptativo porque se comporta de manera sistémica: unidad de propósito, interdependencia de procesos y simultaneidad; es autoorganizado: se reproduce o regenera a si mismo.

FIGURA 6 CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN



Lo más importante las relaciones, lo que hace viable la unidad de propósito son las interacciones, no hay posibilidad de intervenir la seguridad como elemento, sino las relaciones o condiciones globales para lograr que el sistema de seguridad se mueva y se habitúe a lo que la organización quiere, por ello la seguridad por ser una propiedad emergente de estas relaciones es un Sistema Complejo Adaptativo.[17]

[17] Juan Ricardo Morales Espinel, - Pensamiento, generación de conocimiento y aprendizaje en las organizaciones. Universidad de los Andes- Maestria en Redes - Materia Habilidades Directivas II. Bogotá

Los sistemas complejos se comportan de una manera que a partir de una interacción local se genera estructura global emergente, esto es lo que pretendemos interviniendo el elemento personas, lograr estructuras seguras en la tecnología y los procesos.

6.6 SEGURIDAD DE LA INFORMACIÓN: UN VALOR MÁS DE LA CULTURA DE LAS FUERZAS MILITARES

Teniendo en cuenta lo descrito en los capítulos 2 y 3 de la importancia de la seguridad dentro del contexto de las Fuerzas Militares; la propuesta es hacer de la Seguridad de la información un ***valor***, dentro de la cultura corporativa de las Fuerzas, partiendo de la premisa de que corresponde a un concepto ético que tiende a variar en el tiempo, en este caso dependiendo de los cambios y tendencias en la administración de la información y sus tecnologías asociadas; por el momento histórico en el que se vive de integración de nuevas tecnologías, de cadenas de valor que inician y finalizan en los usuarios y que requieren de elementos como la confianza y la seguridad que hagan viable cualquier compromiso laboral, se hace perentorio llevarla a este nivel para lograr trabajarla como un proceso de culturización que brinde efectividad al programa de concienciación en la Seguridad de la Información.

La comprensión de la seguridad de la información como parte de la Cultura Institucional, como un *valor*, una creencia bastante permanente entre lo que es apropiado y lo que no es, sería una guía en las acciones y comportamientos de los empleados para cumplir los objetivos de la Organización en cuanto a Protección de la información en términos de disponibilidad, confidencialidad e Integridad.

Siendo un valor se convertirá en la cualidad que se otorga a la forma de ser y actuar en cuanto a seguridad; la haría deseable como característica propia y de los demás, posibilitando construir un sentido común y una convivencia alrededor de la seguridad de la información.

6.7 METODOLOGÍA PARA CONVERTIR LA SEGURIDAD DE LA INFORMACIÓN EN CULTURA.

La siguiente metodología pretende convertir la seguridad en cultura, de esta manera el ciclo de la seguridad basado en monitoreo, concienciación y aplicado al trabajo diario tendría el siguiente orden analógico:

- Identificar la importancia de la protección de la Información en la misión corporativa, en esos objetivos de orden superior de las Fuerzas Militares.

- Involucrar la seguridad de la información en la filosofía de la Institución, en ese conjunto de principios y valores que la identifican, que haga parte de la forma de pensar de las FF.MM. y contribuya al logro de la misión.

- Convertir la Seguridad en Cultura, aterrizando toda la filosofía de seguridad en acciones concretas a través de hábitos, llevándola al inconciente de cada trabajador. Conformando así la ingeniería del hábito, la infraestructura para crear hábitos; que tiene su origen en la cultura en el inconciente colectivo y su destino en el individuo en el inconciente individual.

Cultura→Conjunto de costumbres→Conjunto de hábitos→Acciones repetitivas se convierten en hábitos→Con tanta insistencia se quedan en el inconciente

- Medir la cultura de seguridad, debe ser medible para ello se deben crear modelos que permitan medir niveles de avance, de cumplimiento, de impacto, de generación de valor, etc.

- Formar los semilleros, los administradores de seguridad que tiene como función liderar el proceso de seguridad de la información con tres responsabilidades básicas brindar conocimiento del tema (qué y para qué), indica que hacer y porque; capacitar (cómo) enseña a hacer las cosas y motivar (querer), es la motivación las ganas de hacer las cosas. Que en otros términos podría ser conocimiento, habilidad y actitud.

- Formar en seguridad de la información a través de programas de fondo, es decir, que muestren la esencia y la importancia de este valor de la cultura institucional a la funcionarios que la conforma, pues ellos son los que hacen la obra; conformando así la ingeniería de la gente segura, creando la infraestructura para hacer empleados con hábitos seguros en la administración de la información. Las premisas de un programa de fondo son:

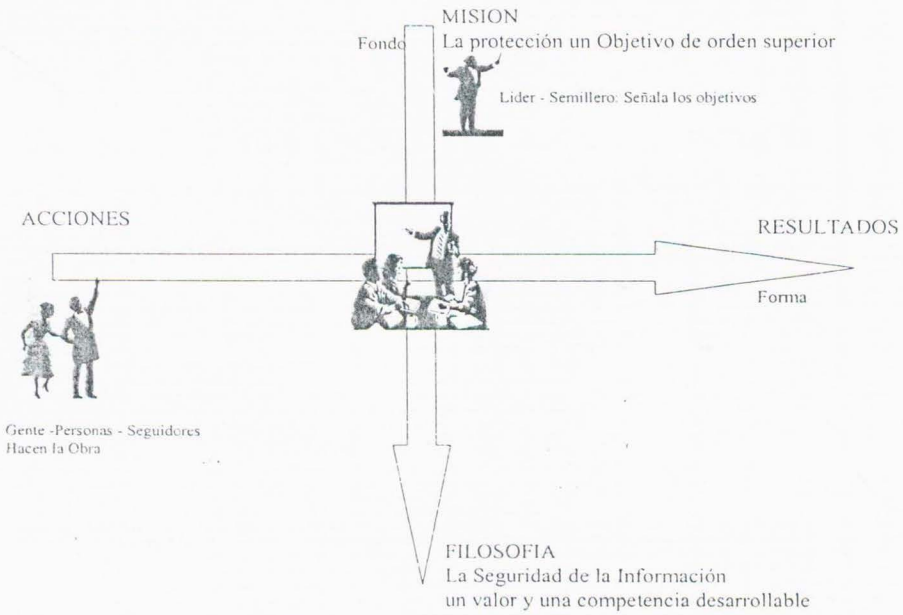
    - *Invierta en el cerebro, en el inconciente colectivo, ahí esta el cambio. A través de las acciones se muestra el fondo, aquellos valores internos, hay que conformar el "Fondo humano de la seguridad", los hábitos seguros en la administración de la información.*

    - *Vender el concepto de seguridad de la información, dar fondo, dar raíces como por ejemplo la seguridad es la base de la confianza y las Fuerzas Militares venden confianza y seguridad a los ciudadanos.*

- *Enseñar valores centrales, que las formas sean la expresión natural de los valores.*

La figura 7, muestra la relación de los conceptos básicos de un programa de formación en seguridad de la información.

FIGURA 7. FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN, UN PROGRAMA DE FONDO



- Crear símbolos, así se cambian inconcientes colectivos. Como por ejemplo: Armando el compromiso con la seguridad de la información, premios a la excelencia en seguridad de la información en el mes de la seguridad en fin.
- Establezca modelos a emular, a través de las analogías.

Esta metodología solo es efectiva si entiende:

- *El cambio de ser y ver es un PROCESO PROGRESIVO: el ser cambia al ver, que a su vez cambia al ser, y así sucesivamente, en una espiral ascendente de crecimiento.*

- *Trabajando sobre el conocimiento, la capacidad y el deseo, se puede irrumpir en nuevos NIVELES DE SEGURIDAD DE LA INFORMACIÓN TANTO PERSONAL COMO INSTITUCIONAL, cuando se rompe con viejos paradigmas y se permite un cambio en los mapas perceptuales y conceptuales.*

¿Cuándo se logra la seguridad de la información en las Fuerzas Militares? Cuando la seguridad es inconciente, cuando hace parte del inconciente de las personas; cuando a través de programas de entrenamiento, se hace tan repetitiva que queda en el inconciente colectivo. Convertida en hábitos, en algo cotidiano.

6.8 CONCIENCIACIÓN DE LA SEGURIDAD Y RESPETO DE LA INFORMACIÓN EN LAS FUERZAS MILITARES

Como se dijo anteriormente, las Fuerzas Militares no son ajenas de una situación que se esta viviendo en el ambiente telemático, al igual que otras instituciones sea concentrado en el hecho de adquirir soluciones informáticas año tras año para subsanar y contrarrestar el problema seguridad informática como es el caso de obtener firewalls, antivirus, IDS, soluciones a nivel de usuarios finales, entre otros.

Pero muy poco se ha hecho con respecto al comportamiento del usuario, más exactamente con la creación de una conciencia de seguridad

informática, que a través de estrategias originen o fortalezcan la cultura de seguridad informática en las Fuerzas Militares, se puede decir que "*con tecnología se puede forzar a un usuario a cambiar su contraseña, pero no se puede hacer nada en los que a su comportamiento refiere... el seguirá anotando el password con un post-it*".

Según los hechos observados durante los últimos años indican que los usuarios, por lo general son el eslabón más débil en la cadena de seguridad; definitivamente en las entidades estatales el funcionario público no entiende como sus acciones pueden impactar en la seguridad de toda la Institución. De igual forma se obtiene que la mayor cantidad de incidentes de seguridad son ocasionados por cosas que hizo o dejo de hacer el usuario.

Asimismo, los funcionarios desconocen su rol y responsabilidad con respecto a la seguridad de la información en las Fuerzas Militares. La mayor cantidad de incidentes de seguridad son generados por el desconocimiento del personal de la Institución, ellos generalmente no saben como reaccionar ante un evento o incidente de seguridad.

6.8.1 Awareness (conocimiento interiorizado o concienciación). Para poder lograr que los funcionarios de la Institución adquieran el conocimiento de la importancia de la seguridad informática, primero es necesario realizar un proceso de "**Awareness" o concienciación**, definido como la herramienta a través de la cual los usuarios reconocen la importancia de la seguridad de la información y los activos de información, se preocupa de forma proactiva y responden de manera adecuada ante cualquier evento o circunstancia que comprometa la seguridad de la informática.

Este proceso busca lograr que los usuarios comprendan su rol y responsabilidad; además, que entiendan que la seguridad de la información

es responsabilidad de todos y que sus acciones pueden impactar de forma adversa en la seguridad de la información.

6.8.2 Triangulo del conocimiento organizacional. *El triangulo del conocimiento organizacional* de la figura 8 representa la estructura que se desarrolla para lograr un proceso de conocimiento adecuado en una organización con respecto a un tema o área, para el caso de la Institución Castrense este triangulo es la base de una implementación exitosa, que facilitaría llegar al punto ideal u objetivo y es la forma adecuada como los usuarios deberían obtener el conocimiento de seguridad informática.

Figura 8 Triángulo del conocimiento organizacional

Se constituye en tres pilares como son el "*Awareness*", el cual como se dijo anteriormente, es el proceso para atraer la atención a la seguridad por parte de los estamentos y funcionarios de la Institución, el "*Training*", cuyo objetivo es desarrollar un entrenamiento adecuado a través de experiencias, tips y competencias, ubica a la Institución en un nivel de

entrenamiento que le permite ser competitivo y lo más importante, estar preparados para enfrentar cualquier tipo de suceso informático. Finalmente, el otro escalón corresponde a la *"educación", herramienta que* permite a la entidad producir especialistas funcionales soportados en el conocimiento especializado para fortalecer lo adquiridos en los niveles anteriores, enriquecidos con la experiencia de los miembros involucrados en el área de la seguridad informática.

Sin embargo este triangulo requiere de unos actores para que se de el conocimiento organizacional, tal como se indica en la figura 9

Figura 9 Triangulo del conocimiento y usuarios

En la gráfica se muestra los actores involucrados en cada uno de los niveles del triangulo del conocimiento, el objetivo es dar a conocer donde van enfocados los diferentes procesos y de esta manera mostrar al alto mando de la Institución quienes están involucrados en los diferentes peldaños.

6.8.3 Obstáculos para el éxito. De acuerdo a las experiencias observadas y analizadas por la Academia Latinoamericana de Seguridad Informática (ALSI) en el momento de implementar metodologías para crear una cultura informática existen varios obstáculos que consideramos convenientes tenerlas en cuenta para que no se repitan en la institución, estas son:

6.8.3.1 Seguridad es un problema de tecnología de información, no es mi problema. Este es la posición de una gran mayoría de usuarios en el cual no quieren involucrarse, precisamente por la falta de conciencia y de conocimiento, esto es lo que más perjudica en el momento de implementar cualquier mecanismo en pro de la cultura informática, **la indiferencia.**

6.8.3.2 Un tamaño ajusta a todos – audiencias. Al momento de implementar una metodología para crear conciencia es importante observar a quien va orientado y cual es la audiencia, no todas las metodologías se pueden aplicar a la Institución, para el caso de las Fuerzas Militares debe mirarse cual es la que mejor se ajusta y puede obtener un mejor resultado.

6.8.3.3 Demasiada información. Por lo general se incurre en el error de generar mucha información durante el proceso de implementación de una solución, que ocasiona confusión en los usuarios participantes y en muchas ocasiones en los mismos implementadores genera traumatismo.

6.8.3.4 Mala Organización. Por el afán de implementar una solución no se cubre los pasos iniciales durante el proceso, ni se asignan responsables de cada actividad, no se da a conocer a todos los estamentos los roles que permiten identificar las responsabilidades. Se hace necesario tomar el tiempo necesario para definir claramente la organización y funciones.

6.8.3.5 Fallas en el seguimiento. En la gran mayoría de los casos se carece de un acompañamiento y seguimiento durante la implementación de una solución y es por ello que muchas veces los esfuerzos se pierden.

6.8.3.6 Llevar el mensaje adecuado al lugar no adecuado. De nada sirve que se desarrolle una buena implementación, excelente campañas de divulgación en el área de seguridad informática, si estas se desarrollan en lugares y sitios en donde no existe un desarrollo tecnológico, por lo tanto no habría usuarios que entendieran el mensaje y muchos menos los apliquen.

Otros obstáculos están identificados en la falta de apoyo del alto mando, la poca disponibilidad de recursos, no explicar el porque de las medidas de seguridad adoptadas ni cual fue la razón que lo origino, se confunde el concepto del término *awareness* con *entrenamiento, así como* algo que la gran mayoría de los usuarios cometen, que es un gravísimo error, es la divulgación de la información confidencial de una manera generosa llamado la "Ingeniería Social".

6.8.4 ¿Cómo resolvemos el problema? El principal obstáculo que impide el éxito organizacional, radica en intentar resolver los retos actuales, utilizando las herramientas del pasado, y esto se da porque se piensa que con el solo hecho de implementar soluciones a nivel de hardware o software, ya se tiene solucionado el tema de seguridad informática, como desafortunadamente las adquisiciones tecnológicas por lo general no se actualizan y muchas veces se vuelven obsoletas con la realidad que se vive en la actualidad.

6.8.4.1 Marketing o Cambio Organizacional. Para poder aterrizar la solución a las diferentes fallas que se encuentran en la Institución en cuanto a la falta de concienciación de la seguridad informática, se requiere implementar una cultura informática que se refleje en hábitos y que conlleve a un cambio organizacional, para ello definimos que marketing o cambio organizacional es el proceso fundamental para la identificación de necesidades y de satisfactores, para finalmente lograr una colocación de los mismos en un mercado.

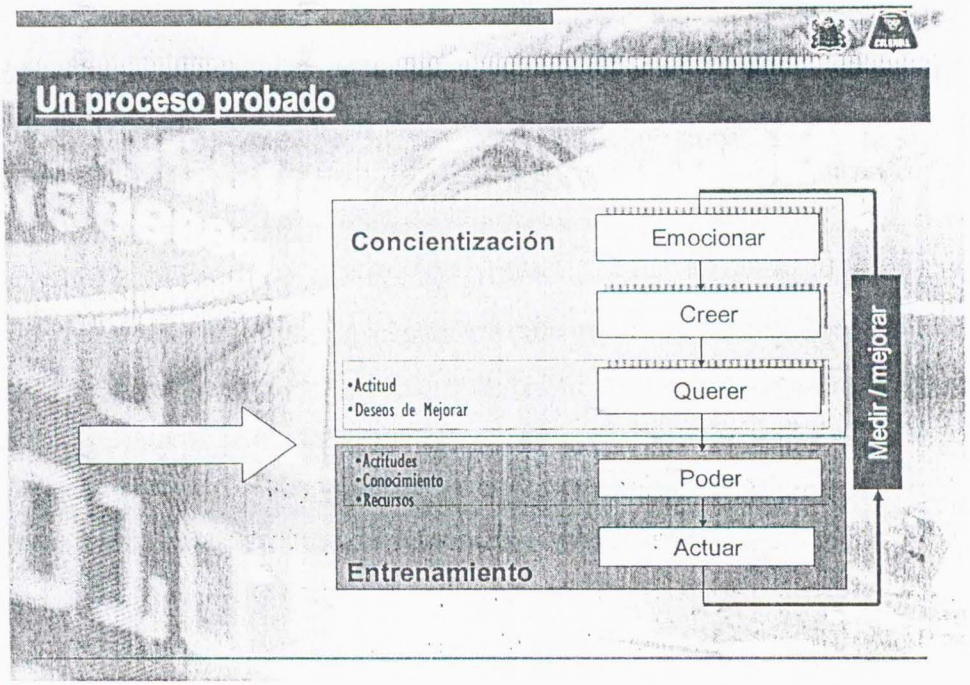
En la visión del marketing, la interiorización de la importancia de la seguridad de la información es nuestro producto o satisfactor, para suplir la necesidad que existe en la Institución. El marketing se considera como una herramienta importante y poderosa para lograr awareness o concienciación en los funcionarios, pero esto no es suficiente, se necesita algo más que marketing para concienciar a las personas ya que buscamos lograr un cambio en su actuar, aptitudes, pensamiento y en la forma de trabajar. En otras palabras, se busca cultura al generar hábitos en la gente para que protejan a la información y que puedan entender que es un activo crítico en la Institución y que si no se cuida, se perdería hasta la razón de ser de la Institución.

Todo esto nos lleva a pensar que el resultado esperado no será una labor trivial, será necesario involucrarse con la forma y cultura de la Institución, con este proceso se van a cambiar practicas de muchos años, por lo tanto existirá personas que se resistan al cambio, y cuando en un proceso de cambio se involucra personas, el riesgo de fracasar es alto.

Por eso la importancia de contar y tener el apoyo del alto mando, porque de ello depende la aceptación tanto del personal superior como del subalterno para el desarrollo y éxito del proceso, tal como se indica en la

Figura 10, la concienciación tiene tres fundamentos importantes como es el Emocionar, Creer y el Querer en donde se requiere actitud y deseos de mejorar por parte de todos los usuarios informáticos de la Institución.

Figura 10 Awareness, es un proceso probado.



Otra parte importante, es la etapa de entrenamiento, donde a partir de los recursos se desarrolla el poder y actuar para realizar labores con base en el conocimiento y experiencia.

Se considera que durante estas dos fases se deben desarrollar indicadores que permitan medir, para así poder mejorar. (lo que no se mide no es susceptible de mejorar). El principal punto de falla se observa específicamente en la carencia de recursos, toda vez que en muchas ocasiones no se cuenta con ello en la cantidad requerida.

6.8.5 Metodología. Para desarrollar una implementación exitosa como ya se ha mencionado, lo primero y más importante es contar con el apoyo del alto mando. Luego, definir el procedimiento para llegar al Awareness adecuado, el cual requiere un conocimiento previo de la cultura institucional, que en el caso de las Fuerzas Militares es entender claramente el funcionamiento, organización y comportamiento que tiene tanto los funcionarios del Ejercito, Armada, Fuerza Aérea y el Comando General de las FF.MM., por lo que las metas y objetivos de este proceso deben ser claros, reales, medibles, comunicables; para luego así crear una estrategia impactante y real a desarrollar.

Por eso la importancia de contar y tener el apoyo del alto mando, porque de ello depende la aceptación tanto del personal superior como del subalterno para el desarrollo y éxito del proceso, tal como se indica en la figura 10, la concienciación tiene tres fundamentos importantes como es el Emocionar, Creer y el Querer en donde se requiere actitud y deseos de mejorar por parte de todos los usuarios informáticos de la Institución.

Para lo anterior, se hace necesario realizar encuestas acerca del estado de la cultura de uso y manejo de la información en las Fuerzas Militares y ponderar las respuestas, darle un peso dependiendo de la importancia que tiene para la Institución, no es lo mismo el uso de passwords débiles que la fuga de información.

Cómo es importante la identificación de la audiencia que va a recibir el programa del awareness y determinar el nivel de conocimiento que tiene sobre la seguridad informática, se debe previamente realizar las encuestas, seleccionar el personal que va ha realizar las encuestas y ubicación de la población al que se le va a realizar la muestra, entre otros.

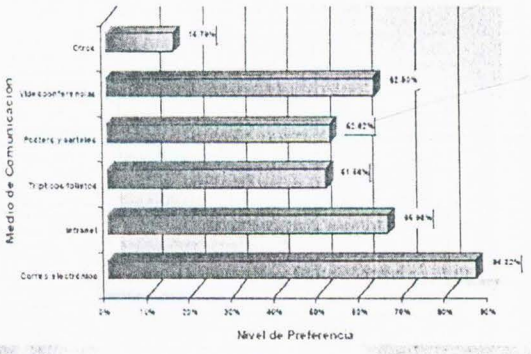
Finalmente, la etapa más importante es la *ejecución y resultados,* en donde se realiza la evaluación de las encuestas, consolidación de resultados, análisis de información recolectada y la elaboración de informe de resultados. Porque con estos resultados se orienta el programa awareness. Ver figura 11 Ciclo para obtención de concienciación y ver ejemplos de resultados en la figura 12.

Figura 11. Ciclo para la obtención de concienciación

Figura 12. Algunos ejemplos de resultados

Metodología de Diagnóstico

- Algunos ejemplos de resultados

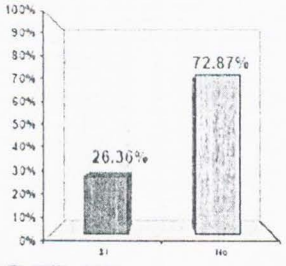


Fuente: Academia Latinoameticana de Seguridad Informática (ALSI)

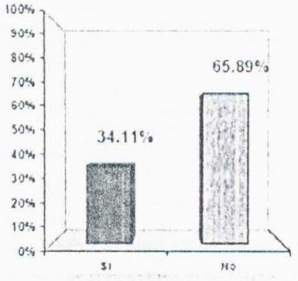
Metodología de Diagnóstico

- Algunos ejemplos de resultados

Los usuarios comparten sus identificadores y contraseñas



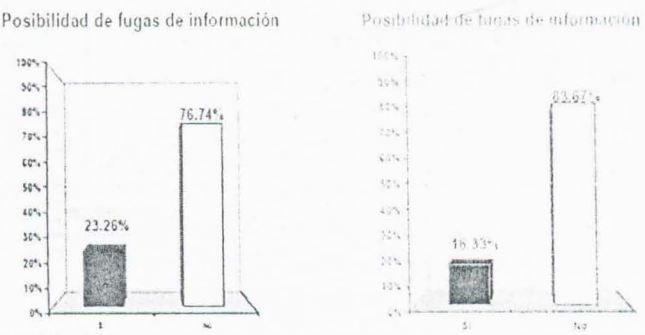
Los usuarios comparten sus identificadores y contraseñas



Fuente: Academia Latinoameticana de Seguridad Informática (ALSI)

Metodología de Diagnóstico

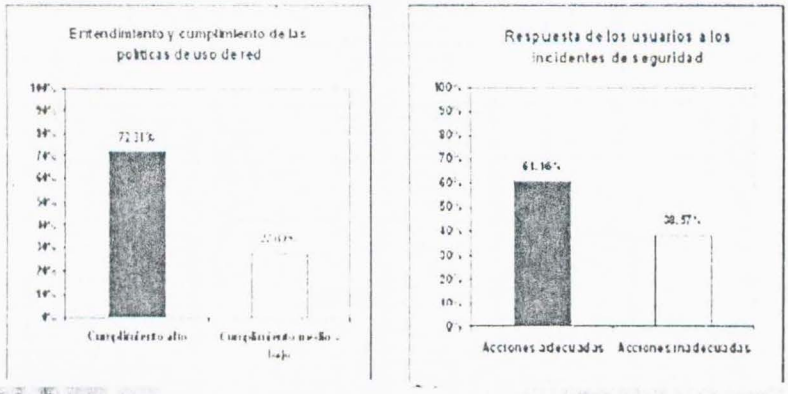
- Algunos ejemplos de resultados



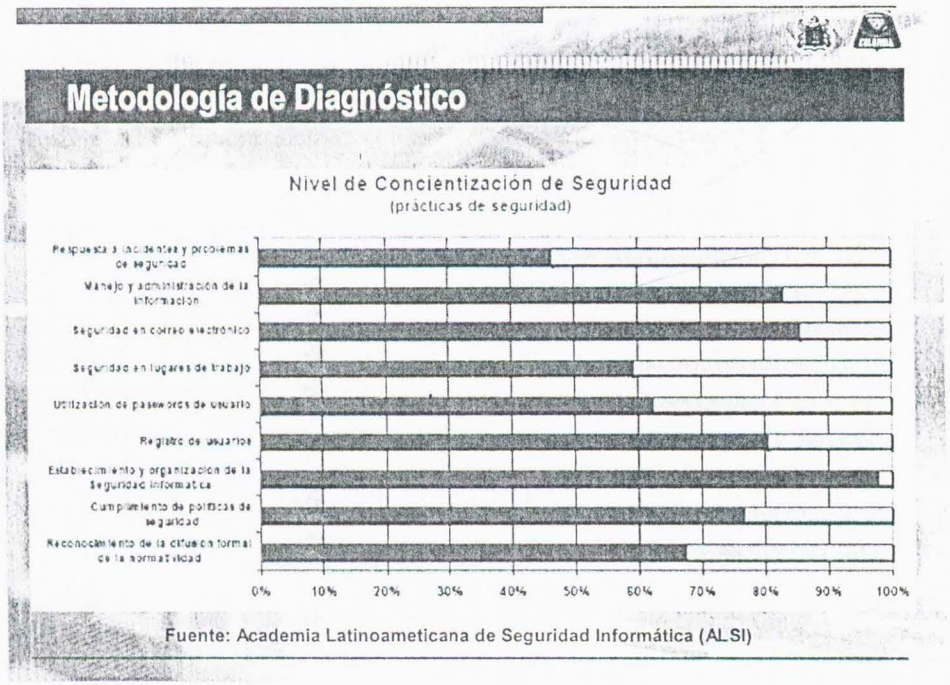
Fuente: Academia Latinoameticana de Seguridad Informática (ALSI)

Metodología de Diagnóstico

- Algunos ejemplos de resultados



Fuente: Academia Latinoameticana de Seguridad Informática (ALSI)



6.8.5.1 Aplicando la Metodología de Awarenes. Una vez se obtenga los resultados consolidados se hace necesario definir una estrategia de awareness considerando la efectividad de los medios, debilidades del conocimiento de seguridad y debilidades en practicas de seguridad del área informática.

Posteriormente, se realiza un análisis y evaluación del riesgo, donde se determina e identifica cuales son los riesgos que se aceptan, cuales son los riesgos que se va a transferir y cuales son los riesgos que se van a contrarrestar y/o mitigar. Luego, se desarrolla el plan de awareness, inicialmente se estructura una campaña de comunicación, la cual consta de una etapa de *pre-lanzamiento*, *lanzamiento y mantenimiento*, *evaluación y reforzamiento*, se debe realizar el esquema del mantenimiento del plan como también establecer cuales son los programas de revisión y mejoras continua del plan.

- **Etapa de Pre-lanzamiento**

  Durante esta etapa se debe seleccionar el tipo de campaña que genere impacto y que cumpla con los estándares de comunicación visual de la Institución, esta puede ser formal es decir en un ámbito ejecutivo o informal a través de dibujos, deportes extremos, etc. Asimismo, se debe seleccionar los medios de difusión de mayor preferencia como son: la intranet, el correo, los poster, a través de las emisoras de la institución, boletines, revistas, entre otros.

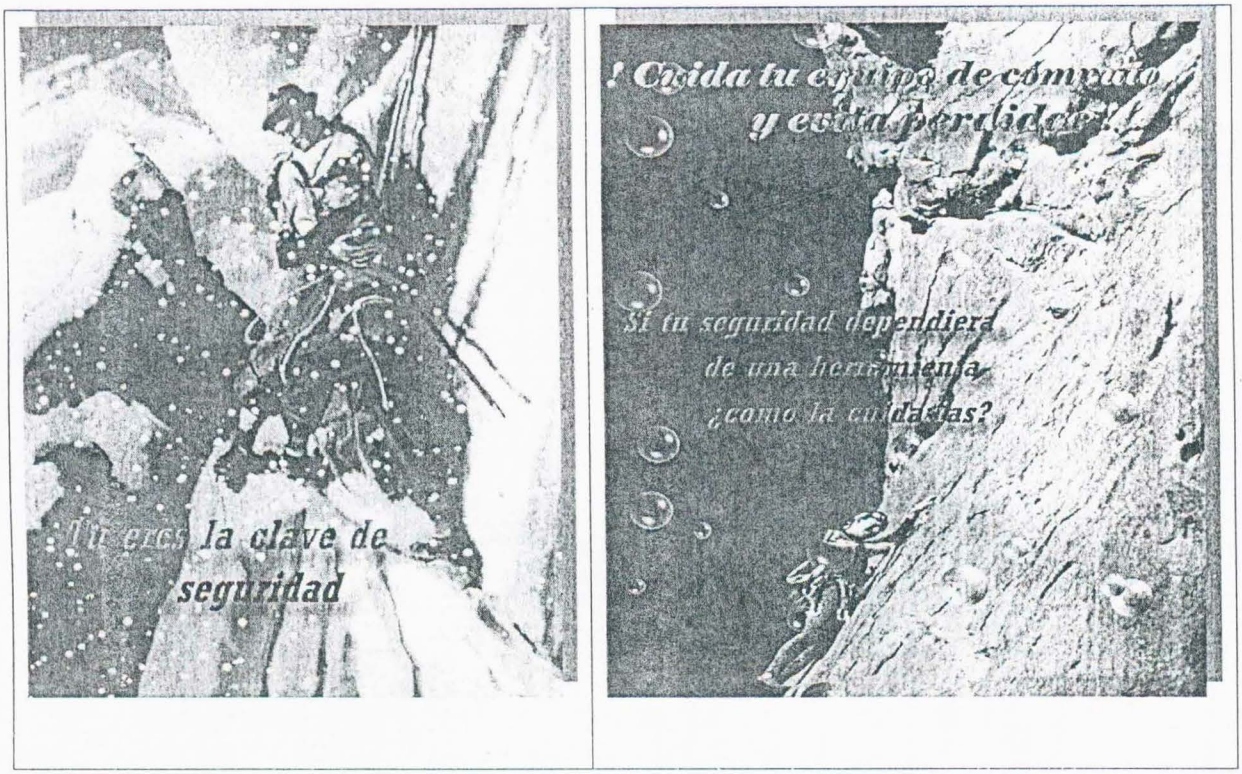
- **Lanzamiento y mantenimiento**

  Algunas fechas que puedan ser usadas como referencia o apoyo son las siguientes:

  - Mayo 10 – Internacional Emergency Response Day.
  - Septiembre 8 – Computer Virus Awareness Day.
  - Noviembre 30 – International Computer Security Day.

- **Algunas mensajes de lanzamiento, pueden ser las que se presentan en la figura 13:**

Figura 13. Poster



- Evaluación y Reforzamiento

En esta etapa muy importante porque permite determinar la efectividad del programa awareness y realizar los respectivos ajustes, aquí también se determina los incidentes de seguridad, para que justar los indicadores que permitan tener una mejor evaluación, esta etapa debe ser continua y flexible que posibilite el ajuste a las nuevas necesidades de la Institución y estar a la vanguardia de la tecnología. Ver figura 14

Figura 14 Otros Afiches

7. CONCLUSIONES

- La globalización conlleva riesgos para la información comercial, dado que cada vez es más frecuente y fácil de transportar, utilizada por empresas en todo el mundo y confiada a terceros.

- Aunque existe un marco que sanciona el uso indebido de la información en las Fuerzas Militares, es necesario generar un enfoque que vaya más allá de lo únicamente punitivo, se debe desarrollar una estrategia integral de manejo y uso de la información por medio de la construcción de una cultura de respeto de la información digital.

- En los funcionarios públicos de las Fuerzas Militares en algunas ocasiones se percibe un comportamiento desinteresado, muchas veces descuidado con "la información" que se maneja en todas las áreas funcionales de la Institución, varias veces tal actitud ha generado sucesos de riesgo en el área informática resultado de la propagación de virus, gusanos y spam, intensificados con el uso del correo y el acceso al Internet indebido.

- En la medida que evolucionan las tecnologías informáticas, se incrementa la necesidad de plantear esquemas claros de protección sobre la información, tal esquema debe enmarcarse dentro del contexto de una metodología de seguridad que trabaje sobre los principios básicos de seguridad: como son la autenticación, confidencialidad, integridad, disponibilidad, control de acceso y auditoria.

- La cultura de seguridad de la infraestructura de informática que se ha venido creado en la Institución se basa en proteger las redes con Firewall, Proxy y

mantener un buen antivirus actualizado en los equipos de cómputo, pero eso no es todo.

- La necesidad de que al interior de la Institución se genere una cultura enfocada a la seguridad permite desarrollar esquemas de control de una forma más participativa, rápida y eficiente. Para llegar a desarrollar una cultura en seguridad informática, es necesario velar porque las políticas de seguridad se transmitan a todas los funcionarios de la Institución, además de contar con el apoyo del alto mando.

- Se puede entender la seguridad de la información a través de las siguientes características: **Confidencialidad, Integridad y Disponibilidad.**

- Las cuatro categorías generales de amenazas o ataques son **Interrupción, Intercepción, Modificación y Fabricación.**

- Una de las tareas más importantes para las FFMM, como parte de la estrategia de seguridad, es crear hábitos en el personal dirigidos al cuidado de la información ya sea confidencial o no, toda vez que esta ligada de una manera u otra con la defensa y seguridad del País.

- Las estrategias de seguridad deben ser sostenibles, duraderas e inteligentes, basadas en soluciones o actividades especificas de acuerdo con las necesidades técnicas reales y a la lógica de la Organización Militar que permitan mantener un adecuado control y administración del riesgo.

- Es fundamental desarrollar una estrategia de concienciación en seguridad (Conocimiento de la Seguridad, llamado como "Security Awareness" en el medio informático), que involucre actividades que tengan como objetivo garantizar que todos los funcionarios públicos de FF.MM. interioricen la

importancia de proteger la información y utilicen las mejores prácticas para su cuidado.

- Las políticas incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad de la información. A menudo estas políticas se pueden acompañar de normas, instrucciones y procedimientos.

- La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes. En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de ingreso, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

- La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes.

- La cultura cumple varias funciones en el seno de una organización. En primer lugar, cumple la función de definir los límites; es decir, los comportamientos difieren unos de otros. Segundo, trasmite un sentido de identidad a sus miembros. Tercero, facilita la creación de un compromiso personal con algo más amplio que los intereses egoístas del individuo. Cuarto, incrementa la estabilidad del sistema social. La cultura es el vínculo social que ayuda a mantener unida a la organización al proporcionar normas adecuadas de los que deben hacer y decir los empleados.

- Antes de iniciar un programa de sensibilización de concienciación de seguridad de la información es necesario implementar una etapa de *Awareness* para garantizar su aplicabilidad y efectividad, seguido del entrenamiento.

- El Awareness tiene como misión transmitir mensajes asertivos para lograr captar la atención de los funcionarios públicos.

- Finalmente, recuerde que toda implementación requiere de indicadores medibles, para que pueda ser mejorado.

- La etapa de Awareness es exitosa cuando tiene la capacidad de marcar una diferencia en el comportamiento y en el hábito de todos los funcionarios públicos, para este caso en la seguridad de la información y cambios en la cultura organizacional.

- ¿Cuándo se logra la seguridad en la empresa? Cuando la seguridad es inconciente, cuando hace parte del inconciente de las personas; cuando a través de programas de entrenamiento, se hace tan repetitiva que queda en el inconciente colectivo. Convertida en hábitos, en algo cotidiano

7.1 RECOMENDACIONES

- Es importante realizar seguimiento y realizar los ajustes durante la implementación a todas las estrategias, políticas y campañas, de tal manera que sea los funcionarios públicos de la Institución se sientan que existe un acompañamiento para lograr su efectividad.

- Se debe exigir que en cada una de las inspecciones que se realicen a través de la Inspección General de cada una de las Fuerzas, se verifique el Tema se Seguridad Informática, donde se verifique los planes de sensibilización que realiza cada una de las unidades, donde conste que todo el personal de la respectiva unidad ha recibido instrucción sobre concienciación de la seguridad y protección de la información.

- Debe incluirse una cátedra en las escuelas de formación de *Seguridad Informática*, para que se garantice que el personal militar que ingresa a la institución conozca la normatividad que rige a la institución en la misma.

- Al personal civil que ingresa a la institución debe realizarse etapas de inducción informática donde se le explique cuales son las condiciones que rige a la institución en temas de seguridad y protección de la información, con la debida constancia que recibieron la información y se compromete a cumplirla.

- De no realizarse etapas de concienciación al personal de la institución cualquier esfuerzo que se haga en materia de protección de la información, será en vano. Porque carece de una habito que le garantice al personal que entiende y son concientes de la importancia de a segura la información.

BIBLIOGRAFÍA

- MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003. P.80.

- Tomado del documento Gestión del talento Humano, Cultura Organizacional. Programa de Formación de Jefes Familia Bolivar. Mayo 2004

- INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION, Comité Directivo de Cobit. Objetivos de Control para la información y Tecnologías Afines. 2ª. Edición. USA, 1998.

- Senge, P. 1995. La Quinta Disciplina. Barcelona: Granica. Citado por MUÑOZ CIFUENTES, Jesús Antonio. Gestión Humana y Planeación: Un reto para la nueva Gerencia de las Organizaciones. Versión preliminar. Bogotá: Uniandes, 2003.

- ESPINEL MORALES,Juan Ricardo - Pensamiento, generación de conocimiento y aprendizaje en las organizaciones. Universidad de los Andes- Maestría en Redes - Materia Habilidades Directivas II. Bogotá.

- HUERTAS, Juan Carlos. Seguridad Corporativa. Revista Sistemas No. 77 p.50.

- GARCIA, Gustavo. Un mundo de Cambios. Revista tecnología de información enero-febrero 2007 p.67.

- http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html 09-Mar-07

- Norma ISO 17799:2005.

- http://www.embarcadero.com/news/press_releases_latinamerica/Seguridad datos-sp.html 14-mar-07

- http://www.sun.com/emrkt/innercircle/newsletter/latam/1206latam_sponsor.html 14-mar-07

- CORTES RAMIREZ, Israel – Integridata. 3 etapa de la academia latinoamerica de seguridad informática.

- QUINTERO SUÁREZ, Adriana Del Pilar. Como asegurar que cada empleado de Seguros Bolivar comprenda su rol y responsabilidad en la protección de la información. Trabajo de Grado Universidad de los Andes. 2004.