Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería
Escuela de Ingeniería Informática

Trabajo Final para optar por el Grado de Licenciatura en Informática con Énfasis en Redes y Sistemas Telemáticos

Tema
Seguridad en la infraestructura de telecomunicaciones enfocado en el entorno Costarricense.

Sustentante: Laura Alfaro Segura
Cédula: 2-0593-038
Tutor: Lic. Miguel Pérez Montero
I Cuatrimestre 2009

La mejor forma de manejar los problemas es evitar que sucedan

INDICE

INTRODUCCIÓN

Las telecomunicaciones se han convertido en pilares fundamentales para las organizaciones, ya que ellas son el medio de transporte de datos que conforman la información necesaria para la operatividad diaria. Las redes ofrecen una gama diversificada de beneficios para las empresas, obteniéndose grandes resultados de producción en vías de desarrollo y mejoras en los procesos.

El acelerado desarrollo del área de telecomunicaciones representa una integración global, permitiendo comunicaciones extremo a extremo en lapsos muy cortos, Internet ha contribuido enormemente con este desarrollo, dando lugar a una nueva tendencia de realizar negocios.

El internet ha marcado una significativa diferencia en la forma de realizar los procesos dentro de las empresas, consiguiendo de esta manera mayores beneficios. Este creciente desarrollo de las tecnologías de información trae consigo situaciones delictivas inimaginables hace algunas décadas atrás, poniendo en riesgo la integridad y funcionalidad de las instituciones.

Entre los inconvenientes más serios se encuentran los fraudes informáticos, debido a deficiencias en materia de seguridad. Las empresas aún desconocen la magnitud del problema al que enfrentan, algunas sufren serias limitaciones e invierten pocos recursos para subsanar dichos problemas, acarreando consecuencias enormes y dejando al descubierto su integridad.

Este problema requiere medidas proactivas, nuevas implementaciones en políticas de seguridad, métodos y dispositivos para combatir la inseguridad en que se encuentran inmersos, la divulgación del conocimiento en temas de seguridad es de trascendental importancia es por ellos que debe ser reforzado, esto unido a procedimientos para disminuir el numero de ataques a las compañías, logrando así conservar la integridad de la información.

El motivo del siguiente trabajo es desarrollar un estudio acerca de la seguridad informática y las generalidades que conlleva.

INTERNET

Internet ha marcado una gran diferencia, revolucionando el proceso de comunicaciones, inicialmente Internet fue creado para el Departamento de Defensa de los Estado Unidos, poco tiempo después al analizar su potencial se convirtió en la interconexión de redes permitiendo la comunicación rápida, ágil y de menor costo a nivel mundial, reduciendo los tiempos de respuesta y otorgando múltiples beneficios.

Internet facilita el flujo de información entre fronteras y permite realizar alianzas globales entre organizaciones, a lo largo de los últimos tiempos se ha venido desarrollando una serie de componentes, aplicaciones y sistemas generando exorbitantes sumas de dinero, facilitando de esta manera el trabajo de organizaciones alrededor del mundo.

La rápida convergencia de los sistemas de tecnología de información ha permitido un acelerado desarrollo en telecomunicaciones, reduciendo considerablemente los costos de operación, favoreciendo el comercio, el desarrollo de nuevas herramientas que contribuyan en la educación, investigaciones científicas, entre otros.

Estos aportes a la humanidad acrecientan el uso de la tecnología y favorecen la interactividad y el alcance global.

A raíz del uso de Internet y como medida para proporcionar seguridad a las compañías se desarrolló la Intranet, mediante sistemas especializados de seguridad, otorgando privacidad a las compañías.

SEGURIDAD INFORMÁTICA

El objetivo principal de la seguridad es la protección de la información, ya que la misma es un activo de mucho valor para las organizaciones, siendo indispensable para la operatividad diaria y sensitiva por la discreción con la que debe ser tratada.

La seguridad de la información se logra implementando una serie de controles que abarcan políticas, prácticas, procedimientos, entre otros con el fin de asegurar la protección de la información de las empresas.

Las fallas en la seguridad implican repercusiones de alto costo económico para la organización, tanto por las pérdidas de la información, el valor de recuperación del incidente, así como las medidas a tomar para prevenir futuros incidentes.

Es esta la razón fundamental para que las organizaciones desarrollen procedimientos enfocados a la seguridad informática que les permita ser proactivos ante eventualidades que atenten con el buen funcionamiento de la institución.

CARACTERISTICAS DE LA SEGURIDAD INFORMATICA

La seguridad brinda protección contra peligro, daño y riesgos que atenten sobre la información de la empresa, el término seguridad involucra una serie de aspectos; la integridad de la información, la confidencialidad, la disponibilidad y el no repudio son los principales fundamentos de la seguridad informática.

La confidencialidad brinda privacidad de acceso a la información, las herramientas informáticas deben proteger al sistema de invasiones por parte de personas o programas no autorizados

La integridad proporciona validez y consistencia de los elementos de información, logrando una sincronización de los sistemas, sin que haya duplicaciones de información.

La disponibilidad permite la continuidad de las operaciones, la seguridad debe garantizar el acceso a la información en el momento que se requiera.

AMENAZAS INFORMÁTICAS

Las amenazas están sujetas a una serie de factores relacionados con las redes, el primer factor se origina mediante un evento, que suele ser una acción que sucede sin distinción dentro de las redes, bien puede ser un intento de conexión, la respuesta de un servidor, un enlace entre diferentes host, entre otros.

El segundo factor son los riesgos, los mismos se originan cuando las vulnerabilidades del sistema son expuestas al entorno mediante los eventos, acá sale a relucir la famosa ley de Murphy “si algo puede salir mal, saldrá mal.”

Un riesgo puede presentarse mediante la presencia de un intruso que intenta acceder a un sistema sin la debida autorización, los intrusos se aprovechan de los huecos en los sistemas o fallas en la programación para ingresar, un ejemplo de esto es la sobrecarga de los enlaces de red (superando la capacidad del disco duro). A los intrusos se les puede categorizar de la siguiente manera:

a) Maliciosos: intención premeditada de ocasionar un daño al sistema, para ello se requiere la violación de la seguridad:

- Funcionarios de la empresa: por diferentes motivos atentan contra la seguridad, ya sean funcionarios de tiempo completo o temporales.
- Hackers: personas que tienen la habilidad de explotar los detalles de los sistemas programables y como extender y explotar sus capacidades, ya sea para algo ético o no.

b) No maliciosos: no media una mala intención sino que sucede por fallas o errores del personal, mediante sus acciones no planeadas pero erróneas ponen en peligro las aplicaciones.

La clasificación de los intrusos se puede apreciar en el siguiente gráfico:

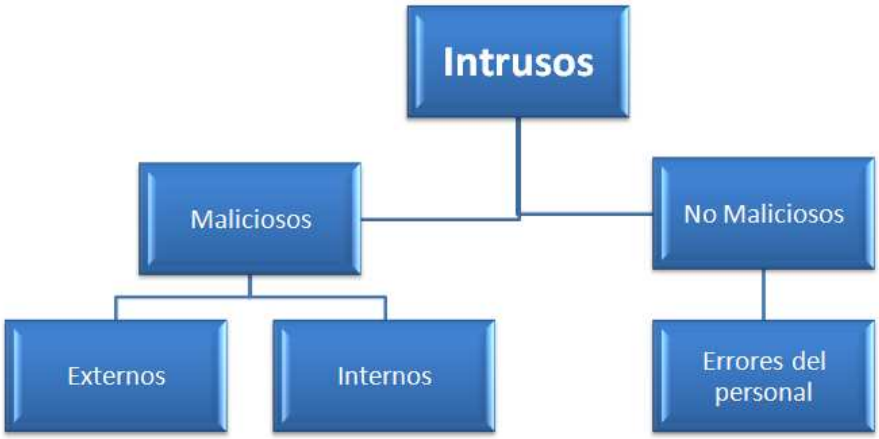

Gráfico 1. Clasificación de los intrusos
Fuente: Confeccionado por el autor

Los ataques dentro de una red corporativa pueden afectar a diferentes componentes, desde el servidor Web, servidor de aplicaciones o archivos, mediante e-mail, portátiles o estaciones de trabajo, para ello se establecen tres momentos cruciales:

- La prevención (antes): es la utilización de diferentes mecanismos que permitan incrementar el nivel de seguridad en el sistema.
- La detección (durante): métodos desarrollados con el propósito de identificar ataques al sistema.
- La recuperación (después) Alternativas que se utilizan y son aplicadas en el momento en que se detecta una incursión al sistema, con el fin de que se retorne al funcionamiento normal.

TIPOS DE SEGURIDAD

La seguridad debe ser implementada desde el diseño lógico de la red, con el fin de evitar problemas de escalabilidad y rendimiento de la red, seguido del diseño físico de la misma, dado el incremento en las conexiones a Internet, Extranet, el comercio electrónico y la nueva tendencia de teletrabajo y usuarios móviles son factores que llevan a ejecutar nuevas medidas proactivas en materia de seguridad.

Las redes empresariales afrontan riesgos latentes que ponen en peligro los activos de las compañías, los riesgos incluyen intrusos externos que violan la seguridad de la red corporativa, usuarios inexpertos que descargan programas o correos con algún tipo de virus.

La seguridad se puede definir de dos maneras; lógica y física, como se detalla a continuación:

1. Seguridad Física

La seguridad física hace referencia a una serie de dispositivos desarrollados para proporcionar el respaldo de la información.

1. Muros de fuego (Firewalls):

Cisco Systems define los firewalls de la siguiente forma:

Permiten bloquear o filtrar el acceso entre dos redes, usualmente la privada y la externa, permiten la conexión segura entre la intranet y el exterior, libre de ataques o virus a los diferentes sistemas organizativos

Un factor importante dentro de los Firewalls es que todo tráfico desde dentro hacia fuera y viceversa debe pasar por donde él, lo cual genera un mayor control de la

red, generando así, que solo el tráfico autorizado definido por la política de seguridad de la empresa sea permitido (p. 810)

Los Firewalls no defienden de ataques o errores de la intranet, de igual manera no ofrecen protección una vez que el intruso los traspasa.

Los firewalls contribuyen a llevar las estadísticas del ancho de banda de las redes por el tráfico de la red, así como los procesos que han influido sobre ese tráfico, de esta manera el administrado de la red puede restringir el uso de estos procesos, con lo que se logra una mejor utilización del ancho de banda.

Los firewalls actúan de acuerdo a los parámetros introducidos por el administrador de la red, por ende si un paquete malicioso no se encuentra definido como una amenaza, lo deja pasar, lo cual se considera una deficiencia, otra limitación es que si un intruso logra entrar a la organización y descubre las contraseñas, el firewall no lo detecta, de igual manera los muros de fuego no proveen filtración de software o archivos infectados de virus, aunque es posible dotar a la máquina donde se aloja el firewall de un sistema de antivirus.

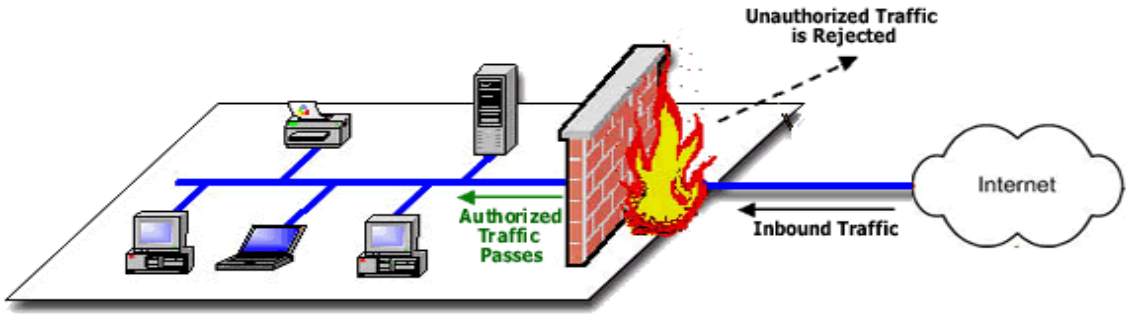

Grafico 2. Ejemplo de un Firewall
Fuente: Tomado de
http://www.aplicacionesempresariales.com/files/2008/06/firewall.gif

En el firewall cada acción que no está explícitamente permitida, su acceso es denegado, sin embargo existen ataques que pueden ser inadvertidos, aun con el uso de este dispositivo, un ejemplo de ello es un funcionario que utilice una Laptop, o un usuario remoto conectado a través de una VPN y que se encuentre en un ambiente de alto riesgo.

2. Seguridad Lógica

La seguridad lógica consiste en una serie de procedimientos que protegen los datos, otorgando permisos para que se pueda tener acceso a la información solo por personas autorizadas.

1. *Sistema de detección de intrusos (IDS):*

*P*ermite detectar actividades inapropiadas, incorrectas dentro de la red de la organización. Suministra información sobre el tráfico malicioso de la red, brindando la posibilidad de detectar intrusiones desconocidas e imprevistas, identifica de donde provienen los ataques.

Los sistemas de detección de intrusos presentan diferentes clasificaciones entere ellas:

- HIDS: operan en un host, informan sobre el estado de un maquina, mediante al análisis de los archivos de la misma, ejemplos de este sistema se encuentran TripWare, Syslog (Server Logs) entre otros.

- NIDS: monitorea los paquetes de la red y los examina en comparación con las reglas preestablecidas, ejemplo de este sistema; Snort, ISS Real Security, entre otros (Vincent Alapont 2002).

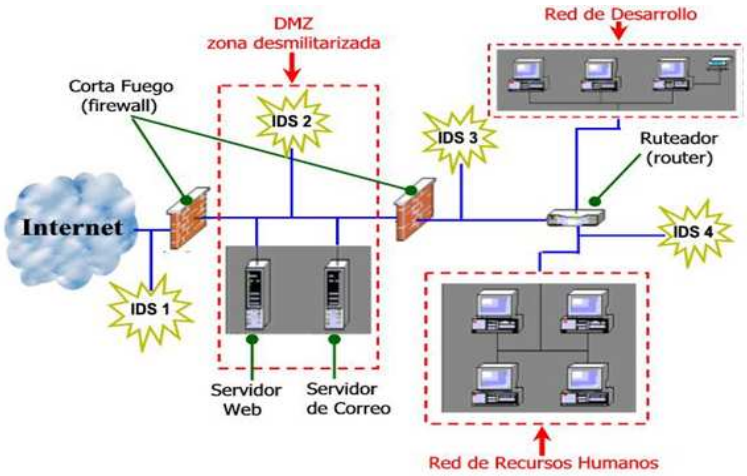

Gráfico 3.sistema de detección de intrusos
Fuente: Tomado de http://www.uv.es/montanan/redes/trabajos/IDSs.ppt#274,19

Un IDS reporta y detecta intentos no autorizados al sistema, filtra y analiza el tráfico que pasa a través de un punto de la red específico.

2. *Sistema de Prevención de intrusos (IPS):*

Pueden bloquear en forma pro-activa todas las conexiones sospechosas que puedan presentarse en el sistema, son capaces de detectar y bloquear automáticamente el tráfico, operando en tiempo real y con un menor impacto para el sistema (Arturo de la Torre, 2006).

Este método varía de los muros de fuego en que representan una mejora tecnológica, ya que son capaces de tomar decisiones de control de acceso basado en los contenidos del tráfico de la red, en lugar de direcciones IP o puertos.

Un IDS alerta a los administradores sobre detecciones de intrusos, mientas que el IPS, establece políticas de seguridad para proteger a un equipo, esta es la diferencia más significativa entre ambos métodos

3. *ISA Server*

Es un Gateway integrado de seguridad perimetral que protege frente a amenazas, otorgando la posibilidad de conexión remota de manera segura. Es una tecnología desarrollada por Microsoft (Microsoft, 2006).

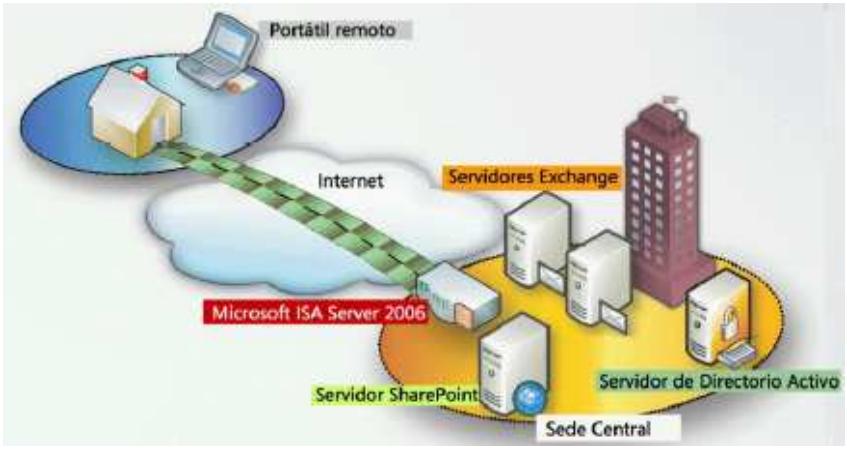

Gráfico 4. ISA SERVER
Fuente: Internet Security acceleration Server, Microsoft 2006.

MÉTODOS DE AUTENTICACIÓN

1. *Identificación y autenticación:*

Permite prevenir el ingreso de personas no autorizadas, la identificación se da cuando el usuario se da a conocer en el sistema y la autenticación es la verificación que el sistema realiza sobre esa identificación (Cisco Systems 2004).

2. *Asignación de Password (Contraseñas):*

Se utiliza para realizar la autenticación del usuario, con el fin de proteger los datos y las aplicaciones, una de las debilidades que presenta este aspecto es la selección de contraseñas frágiles por parte del usuario, dado lo anterior se debe definir el periodo mínimo que debe pasar para que los usuarios cambien sus contraseñas y un período máximo que puede transcurrir para que estas caduquen (Cisco Systems 2004).

3. Cifrado de datos:

Cisco Systems define el cifrado de datos de la siguiente manera:

Brinda confidencialidad de los datos, consiste en dos enfoques; mezclar los datos para protegerlos de su lectura por alguien que no es el receptor esperado e Identificar el remitente de los datos. El cifrado de datos se implementa en organizaciones que utilizan redes privadas virtuales (VPN) (P. 808).

El objetivo del uso de cifrado de datos es utilizar claves para descifrar los datos, una clave secreta es aquella que no permite a los intrusos interpretar la información, cuando un emisor y un receptor utilizan las misma clave se conoce como clave simétrica.

4. Listas de Control de acceso (ACL):

Se aplican a la interfaz del router, son una serie de instrucciones que otorgan o deniegan permisos, mediante ciertas especificaciones, como la dirección de origen, la dirección de destino y el número de puerto.

Permiten denegar el acceso no deseado a la red, a diferencia de otros métodos y sistemas, las ACL otorgan flexibilidad de filtrado básico del tráfico, un ejemplo de esto es el bloqueo de páginas Web, a través del puerto correspondiente.

5. *Control de admisión a la red (NAC):*

Protege a las empresas a través de la autenticación, autorización, evaluación y recuperación de equipos de usuarios remotos conectados, tanto mediante accesos inalámbricos, como a través de la red fija, antes de concederles acceso a redes corporativas.

"La integración de NAC dentro del routing simplifica la complejidad de las operaciones para nuestros clientes, y ofrece una solución única ", dijo Mick Scully, Vicepresidente de Administración de Productos en el Grupo de Tecnología de Seguridad de Cisco. "En la medida en que las empresas soportan más dispositivos, NAC Profiler fortalece la habilidad de las tecnologías de la información para proteger tanto a usuarios como a dispositivos, sin la necesidad de agregar otro servidor. Cisco está ampliando y profundizando la capacidad de la IT para proteger a las empresas, a sus empleados y a la información" (Cisco INTEGRA 2007)

POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad de una organización nacen con el fin de crear conciencia en los diferentes funcionarios de la importancia de proteger la información, es por ello que la creación de una política de seguridad implica un alto grado de compromiso, tanto del área gerencial como de los diferentes funcionarios

La definición de una política de seguridad implica un exhaustivo análisis de los diferentes procesos de la organización, con el fin de identificar fallas y debilidades en los mismos. Para mantener las políticas de seguridad actualizadas se requiere de esfuerzos y mejora continua, con el propósito de afinar conceptos y actualizar detalles.

CISA 2001 hace referencia a la política de seguridad bajo los siguientes términos:

> La política contribuye a la protección de los activos de la información, su objetivo es proteger el capital de información contra todo tipo de riesgos, tanto accidentales como intencionales. Una política de seguridad de sistemas robusta que exista y aplique es de suprema importancia para la supervivencia y el desarrollo de una organización. La política debe asegurar que los sistemas se ajusten a las leyes y regulaciones, a la integridad de los datos, además de la confidencialidad e integridad.

Para definir una política de seguridad es requisito fundamental apegarse a los objetivos de la institución, dependiendo del nivel de cultura de la organización, así debe determinarse las medidas para su correcta implantación y difusión, estableciendo de vías eficaces para la comunicación.

Existen factores claves en la para la definición de las políticas de seguridad, en primera instancia la valoración de los activos de la organización, su nivel de importancia y criticidad, unido a lo anterior se deben identificar y analizar las amenazas que atenten contra los activos, estimación de las vulnerabilidades en términos de probabilidad de ocurrencia e impacto, en caso de materializarse la amenaza.

Para evaluar los procedimientos inmersos en la seguridad informática dentro de la organización, se realizan auditorías, el cual es un procesos evaluativo que determina controles y realiza una medición del funcionamiento, con el fin de determinar posibles inconsistencias y tomar las medidas pertinentes, para garantizar el cumplimiento de los fundamentos de seguridad antes descritos.

The American Accounting Association lo define claramente como “El proceso sistemático para evaluar y obtener de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados”. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando los principios establecidos para el caso”.

Para realizar las auditorías se utiliza el Estándar Internacional de auditoría de sistemas de información ISACA (Information Systems Audit and Control

Association), unido con el Marco Referencial de COBIT, así como la norma ISO 17799-2000.

Existen otras normas Internacionales para la Seguridad, las cuales se citan a continuación, las mismas son insumo importante tanto para la definición de las políticas de seguridad, así como para llevar a cabo las auditorías, las mismas son moldeables a la organización y es responsabilidad de las autoridades correspondientes determinar cuál reúne las características necesarias acorde a sus necesidades.

Normas Internacionales

- ISO177799
- BS7799
- ISO9001
- COBIT AUDIT GUIDELINES
- COSO
- ITIL
- SARBANES OXLEY ACT

DELITOS INFORMÁTICOS

Las computadoras representan un medio eficaz para la obtención de información, la informática está presente en diversos campos de la vida moderna, revolucionando la forma de trabajar y automatizando procesos que antes se realizaban de forma manual.

El creciente progreso en materia computacional permite procesar y poner a disposición de las sociedades exorbitantes cantidades de información de toda naturaleza, sin limitante alguna, de fácil y rápida entrega, sin embargo es la misma evolución de la tecnología lo que acarrea un problema consigo, el mal uso de la información, de los sistemas, para atentar contra el buen operar de las comunicaciones.

En los primeros tiempos los ataques involucraban poca sofisticación técnica, ciertas personas utilizaban sus permisos para modificar archivos, o los entes externos ingresar al sistema averiguando el password del mismo, sin embargo, con el paso de los años estas técnicas se han perfeccionado.

Se podría definir el delito informático como toda acción (u omisión) culpable, realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena.

Los delitos informáticos involucran una serie de actividades criminales tales como robos, hurtos, fraudes, sabotajes entre otos. Los delitos informáticos involucran la alteración del funcionamiento normal de un sistema informático mediante virus, la intervención de líneas de comunicación, entre otros.

En Costa Rica existe la ley No. 8148, promovida por la Asamblea Legislativa de la República, en los siguientes artículos:

> Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.
>
> Artículo 217 bis.-Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."
>
> Artículo 229 bis.-Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Son rescatables los esfuerzos que el gobierno ha realizado en materia de Seguridad, esto evidencia la importancia que nuestras autoridades gubernamentales estiman en materia de Seguridad Informática.

El martes 11 de noviembre del año 2003 se publico en el diario la Gaceta el decreto Nº 31435-MICIT, establecido por El PRESIDENTE DE LA REPÚBLICA Y EL MINISTRO DE CIENCIA Y TECNOLOGÍA que determina lo siguiente:

"Ley de Promoción del Desarrollo Científico y Tecnológico" Nº 7169, del 26 de junio de 1990.

Considerando:

1º—Que es importante para el país conocer que los problemas y soluciones de seguridad que se presentan en aplicaciones tecnológicas de la actualidad.

2º—Que las tecnologías de información se han convertido en el vehículo que permite la mejora de los servicios tanto para el sector público (gobierno digital) como para las organizaciones privadas y la temática de la Conferencia se orienta a cómo estos servicios pueden ser mejores.

3º—Que se debe contar con servicios de calidad en el área de tecnologías de información con lo cual es importante para que el país mejore su competitividad a nivel internacional y por lo tanto se estimule la inversión de empresas importantes en Costa Rica. La II Conferencia de Seguridad Informática & Continuidad de Negocios (INFOSECLA 2003) tiene como uno de sus objetivos promover que los servicios en tecnologías de información estén acordes a los estándares internacionales de calidad.

4º—Que la II Conferencia de Seguridad Informática & Continuidad de Negocios (INFOSECLA 2003) es un medio ideal contar con la presencia de expertos internacionales que comparten sus experiencias en países desarrollados y por lo tanto estimular la búsqueda de mecanismos que impulsen el mejoramiento de los servicios en tecnología de información y su seguridad tanto en empresas públicas como privadas. Por tanto:

DECRETAN:

Artículo 1º—Se declara de Interés Nacional la II Conferencia de Seguridad Informática & Continuidad de Negocios (INFOSECLA 2003), la cual se realizará del 27 al 29 de octubre del año 2003.

Artículo 2º—Se insta a todas las instituciones del Estado, para que en la medida de sus posibilidades y dentro del marco normativo vigente apoyen a esta actividad.

Artículo 3º—Rige a partir de su publicación.

Dado en la Presidencia de la República.—San José, a los veintidós días del mes de setiembre del dos mil tres.

ENTORNO COSTARRICENSE

La creciente evolución en el área de telecomunicaciones ha impactado fuertemente al país, enfocado en dos grandes áreas; el sector privado, el cual se constituye por tener pequeñas y medianas empresas, así como grandes compañías de un gran dominio internacional, que han plantado sus bases en nuestro país y que son fuente de grandes divisas, con tecnologías de punta, por otro lado se encuentra el sector gobierno, con entidades públicas, instituciones descentralizadas, así como entidades autónomas y demás poderes de la República.

1. *Sector Privado*

Las PYMES (pequeñas y medianas empresas) del sector privado, representan un gran auge en el uso de la tecnología, depende en gran medida del tamaño de la empresa y la ubicación geográfica de la misma, sin embargo los esfuerzos del gobierno hacia este sector han sido muy significativos, creando parques industriales y promoviendo el sector costarricense como fuente importante para implantar empresas, dadas sus condiciones a nivel de personal capacitado, subsidios entre otros.

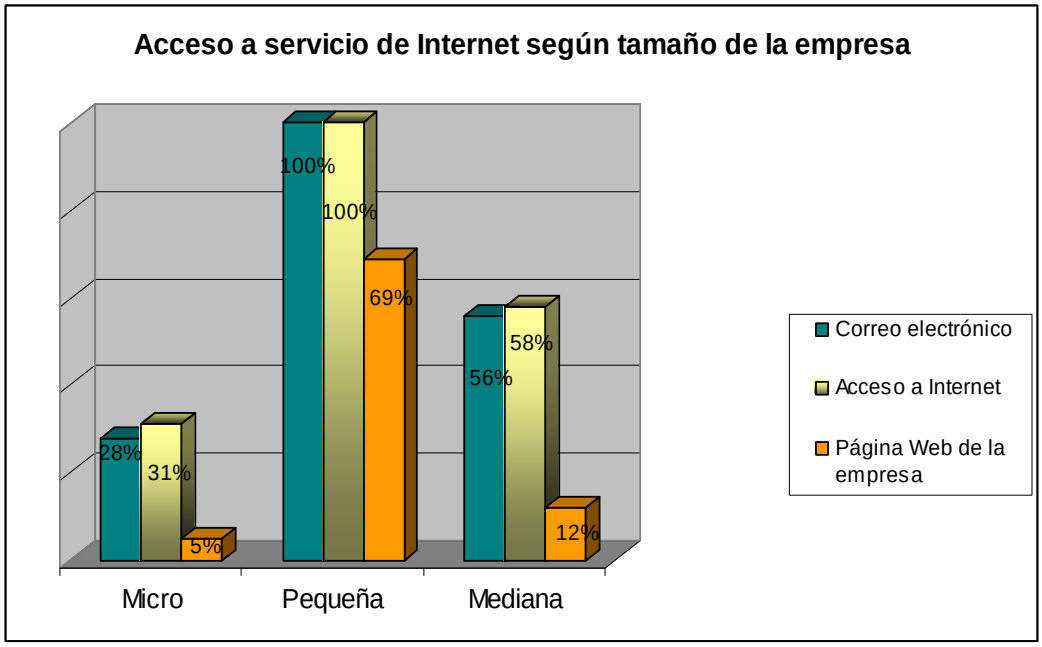

Grafico 5 Acceso a servicio de internet según tamaño de la empresa
Fuente: Encuesta del MICIT realizada a 167 PYMES

El gráfico anterior visualiza el porcentaje de acceso con el que cuentan las PYMES en Costa Rica, dejando en evidencia el gran porcentaje de acceso a Internet, por parte de las mismas.

Entre las barreras que se presentan en el uso de las tecnologías de información para las PYMES, figura el alto costo de implementación, soporte, mantenimiento y actualizaciones, el corto ciclo de vida de los sistemas, dada la inversión que representan, sin embargo, un factor de gran relevancia es el caso de

la seguridad, muchas empresas consideran que realizar sus operaciones mediante Internet, es insegura, como se evidencia en el siguiente gráfico.

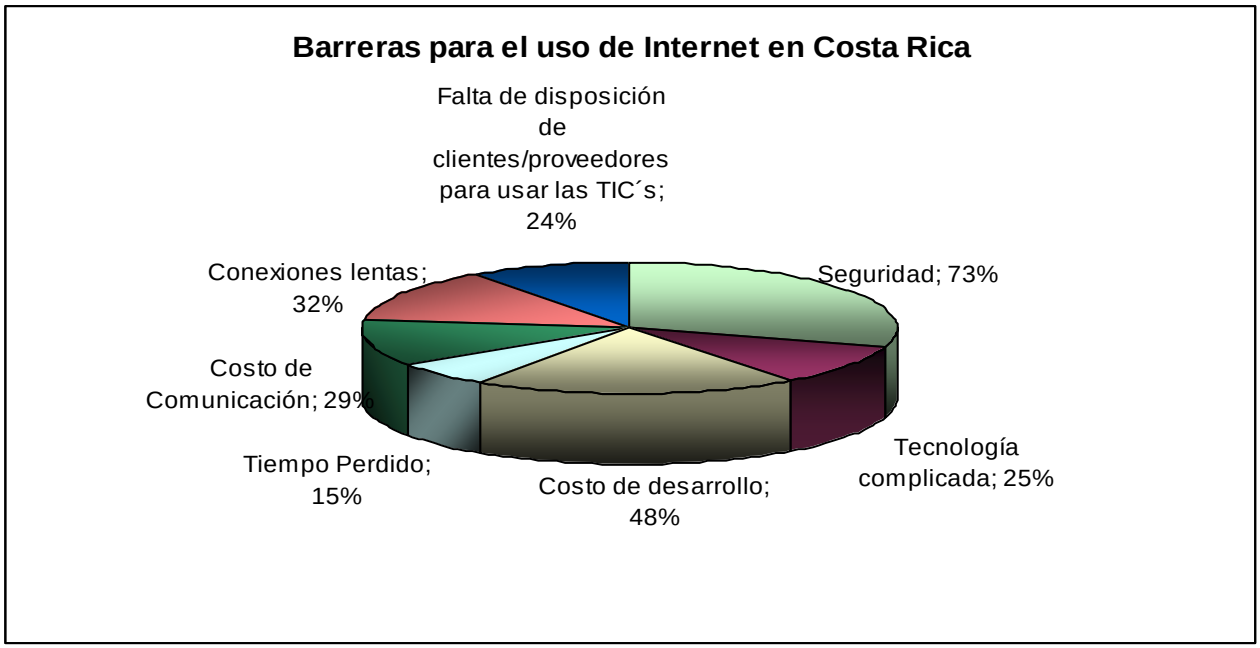

Gráfico 6. Barreras para el uso de Internet en Costa Rica
Fuente: E-Commerce and Development Report 2004, United Nations Conference on Trade and Development

2. Gobierno Nacional

Este artículo se enfoca en el sector público, pues el mismo representa el patrimonio de todos los costarricenses, dando así un panorama general de su evolución y uso en el campo tecnológico.

Es responsabilidad de las autoridades gubernamentales promover el uso de las tecnologías de información, facilitando las comunicaciones entre instituciones y ciudadanía en general, así como determinar las iniciativas que se desarrollen en materia de gobierno digital. “Configurar el Gobierno Digital de manera tal que haga transparente la gestión pública y posibilite nuevas formas de interacción de la

ciudadanía con las instituciones; así como realizar transacciones a efectos de agilizar la prestación de servicios". (Gobierno digital, 2006)

Dentro del sector gobierno el ambiente es muy prometedor, ya que en su totalidad la gran mayoría de las instituciones cuentan con acceso a Internet, conforme pase el tiempo mas funcionarios cuentan con acceso a Internet y requieren del mismo para realizar sus labores cotidianas. En el siguiente gráfico se muestra la situación para los funcionarios públicos, evidencia que se requiere de mayores esfuerzos para incentivar el uso de la tecnología.

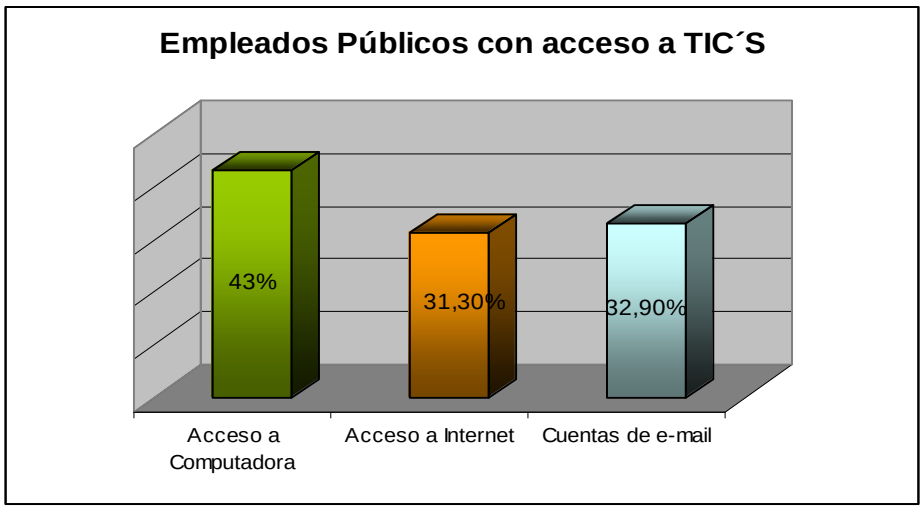

Grafico 7.

Empleados públicos con acceso a TICs
Fuente: Encuesta CONATIC-MICIT 2006

Es necesario establecer las medidas respectivas en materia de seguridad, con el fin de reducir la vulnerabilidad de las empresas e instituciones públicas, estableciendo políticas de seguridad con el fin de reducir los ataques para evitar los daños.

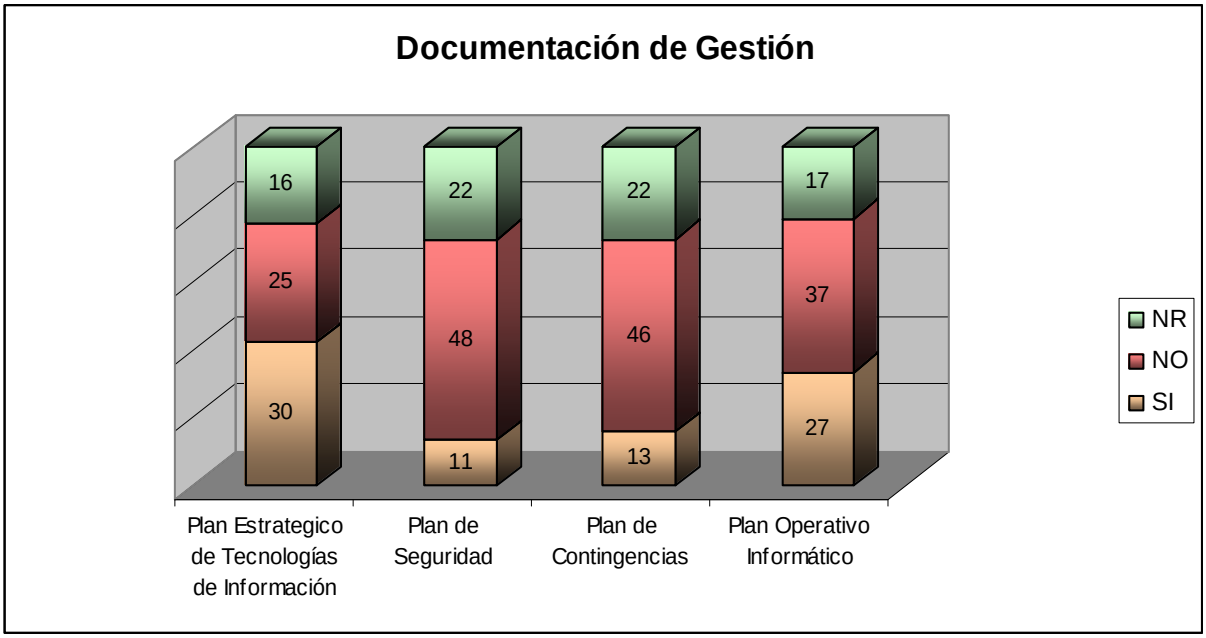

Gráfico 8. Documentación de Gestión
Fuente: Encuesta CONATIC-MICIT 2006

Es necesario establecer planes de seguridad informática que satisfagan las necesidades del entorno nacional, definir claramente planes de contingencia en caso de ataques o problemas en los sistemas, esto reduce el tiempo de respuesta y recuperación ante una eventualidad.

Los resultados visualizan que de 81 instituciones encuestadas, solamente el 8% cuenta con un plan de seguridad informática definido y un 10% posee planes de contingencia, lo que la encuesta no evaluó es si las empresas que cuentan con el plan de informática realizan una implementación del mismo y lo tienen debidamente actualizado según las demandas del negocio, este último aspecto es fundamental, para que los esfuerzos no sean en vano.

El sector gobierno sufre serios limitantes, para el buen manejo del uso de las TIC's, principalmente la poca inversión que se realiza en materia tecnológica, la falta de capacitación en el personal, el grave problema de mantener el personal capacitado, pues la mayoría decide incorporarse al sector privado, dado los beneficios económicos y remuneraciones que proporcionan.

Esto evidencia la necesidad de optar por medidas de seguridad que garanticen la buena operatividad de las funciones.

3. Seguridad en el Entorno nacional

Ante la gran problemática en la inseguridad de las aplicaciones que acarrea al entorno nacional, el gobierno ha promovido diferentes tecnologías con el fin de minimizar los ataques y otorgar seguridad a la información de la empresa, velando de esta manera por el cumplimiento de los fundamentos de la seguridad.

Un nuevo concepto difundido por el Gobierno Digital es el de ciudad "inteligente" o "digital" refiriéndose a una comunidad que promueve e impulsa la Sociedad de la Información en los diversos ámbitos (educativo, cívico, cultural, social, laboral, económico, productivo, sanitario, entre otros), a través del uso de tecnologías de información y comunicación (TIC) (Gobierno digital, 2008).

No es posible concebir un creciente desarrollo en el área de informática, si no se provee de una adecuada seguridad para el correcto funcionamiento de los procesos, para ello se promueve mediante la ley 8454 el uso de la firma digital.

Durante la administración del Doctor Pacheco se publicó la LEY 8454, Ley De Certificados, Firmas Digitales y Documentos Electrónicos, la cual rige a partir de su publicación, fecha de vigencia: 13/10/2005 (Nº Gaceta: 197 del: 13/10/2005).

Como lo establece la Ley 8454:

> *Entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.*
>
> *Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.*

Existen ciertos requisitos que las empresas, tanto públicas como privadas deben cumplir con la finalidad de implantar un modelo de firma digital, entre ellos:

- Requisitos a nivel de hardware y software necesarios.

- Jerarquía de Autoridades Certificadoras (CA), CA Raíz, CA Intermedio, CA Emisor.

- Cumplir con normas internacionales, supervisadas por el Ministerio de Ciencia y Tecnología (MISIT), mediante LA Dirección De Certificados de Firma Digital y el Ente Costarricense de Acreditación (ECA).

- Existen otras normas internacionales como la Norma ISO 21188, que establece una serie de controles, enfocados en el aspecto físico, responsabilidades del personal, ciclos de vida de certificados, entre otros.

Certificados digitales: es un documento electrónico que relaciona una identidad con una Llave Pública. El certificado digital es emitido por una Autoridad Certificadora, quien define un procedimiento de certificación de identidad, con el que se prueba la autenticidad, a partir de ello se genera un pare de llaves criptográficas, de esta manera se crea un certificado digital, el cual se firma con la llave privada de la autoridad certificadora.

En Costa Rica se planteó un modelo que se resume de la siguiente forma:

1- Definir una única Entidad Certificadora Raíz.

2- Cumplimiento de las directrices del ente costarricense de acreditación (ECA).

3- Aprobación de las políticas por la autoridad correspondiente, en este caso PAA.

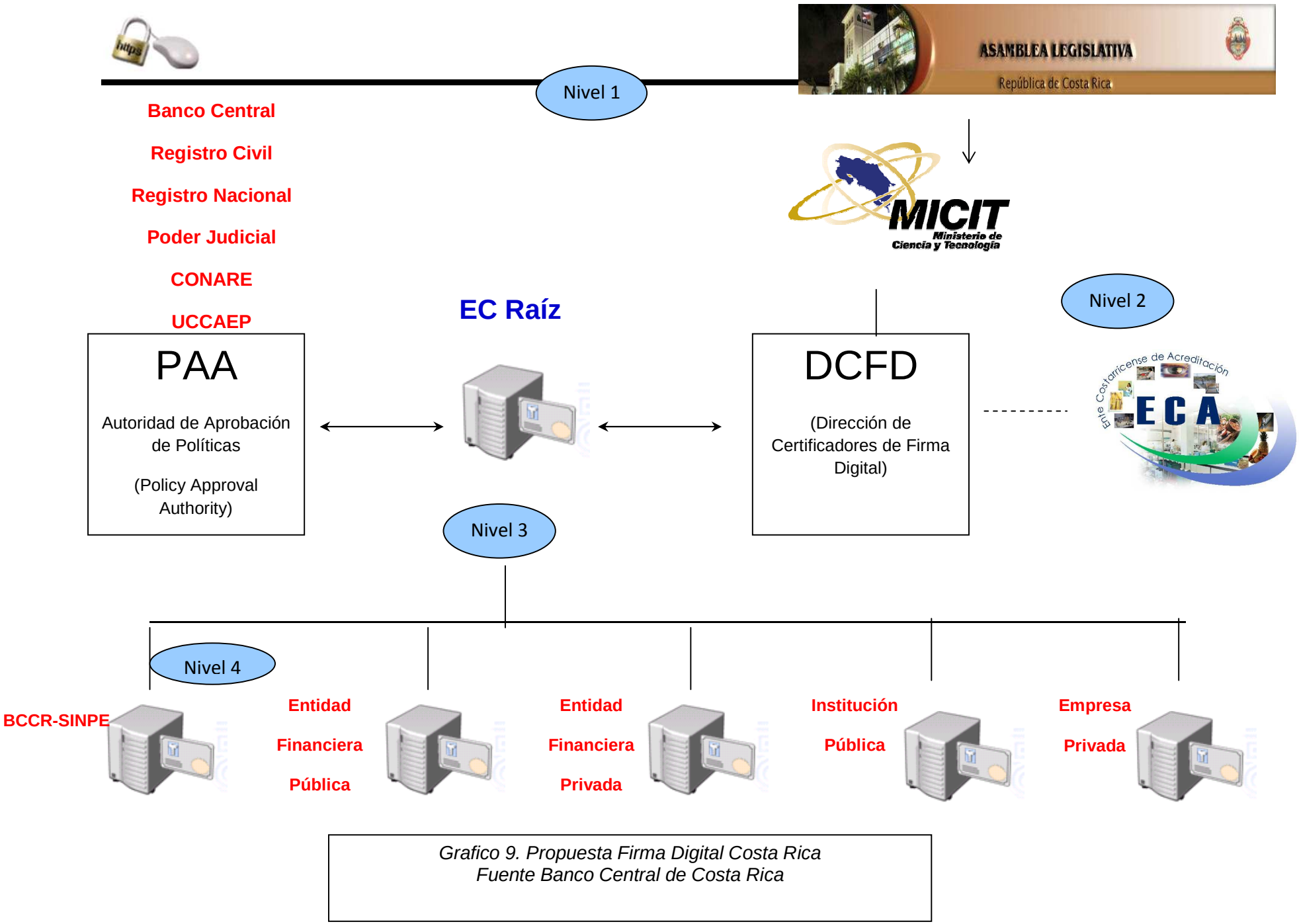

Grafico 9. Propuesta Firma Digital Costa Rica
Fuente Banco Central de Costa Rica

Con el fin de satisfacer demandas dentro del territorio nacional, se han llevado a cabo una serie de proyectos tecnológicos, necesarios para responder a las necesidades de la ciudadanía costarricense, mejorando y automatizando procesos, facilitando de esta manera la ejecución de ciertas actividades.

Proyectos de impacto nacional como SINPE (Sistema Interbancario Negociación y Pagos Electrónicos), Compra RED (sistema de automatización de contratación administrativa), TICA para el sector aduanero y actualmente desarrollando Tributación Digital, entre otros.

Estos proyectos por su impacto nacional, nivel de complejidad, calidad en el servicio brindado, así como la confiabilidad, deben utilizar métodos de autenticación, que permitan la protección de los datos que contienen, a raíz de la ley 8454, se establece el uso de firma digital para los anteriores proyectos, como ejemplo de ello se describen el siguiente gráfico el proyecto SINPE, debido a la gran cantidad de usuarios que utilizan el mismo para realizar sus transacciones bancarias vía Web (aproximadamente 500.000 usuarios).

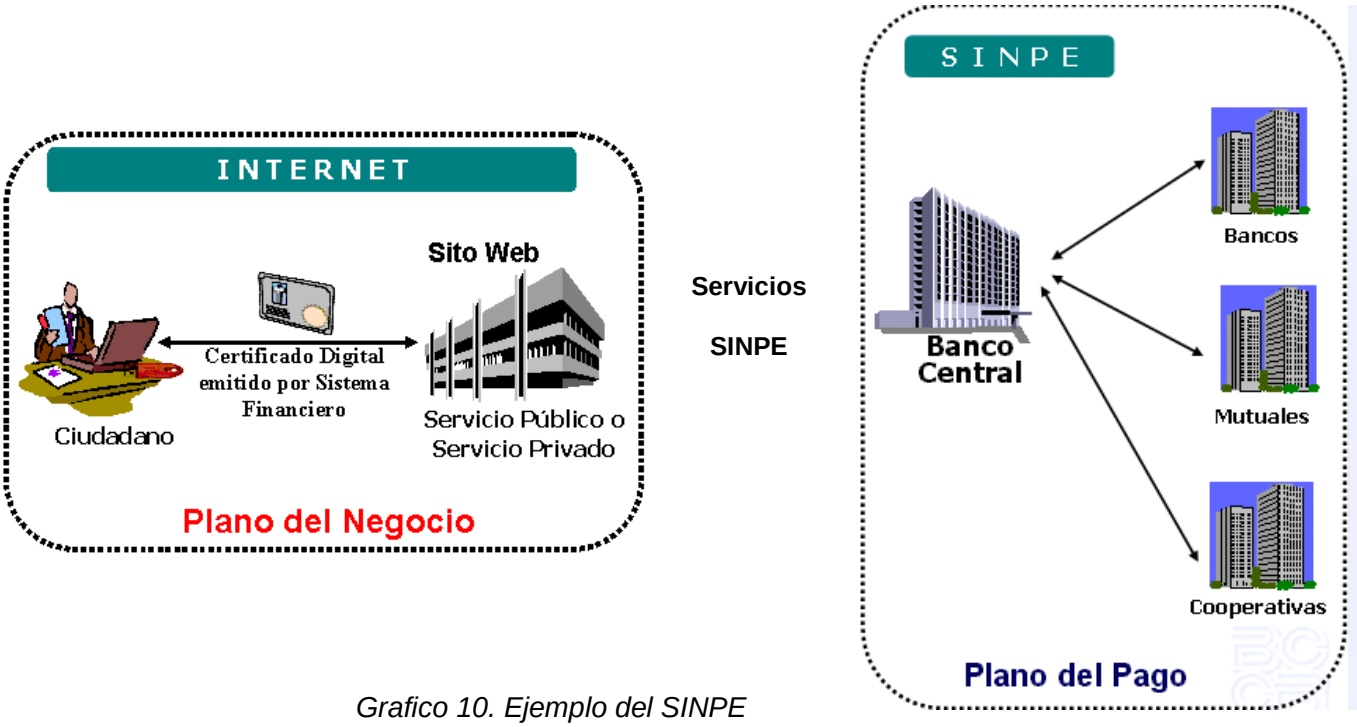

Grafico 10. Ejemplo del SINPE
Fuente: Banco Central de Costa Rica

El Banco Central determina los siguientes roles:

Para el Banco Central:

- Construir la infraestructura de la Autoridad Certificadora Raíz dentro del Banco Central, estructura de la Dirección de Certificados de Firma Digital para las Autoridades Certificadoras acreditadas por el Ente Costarricense de Acreditación.

- Desarrollar el proyecto Firma como un servicio del SINPE, siendo esta la Autoridad Certificadora del sector financiero costarricense.

- Reglamentar el servicio Firma como parte de las regulaciones del Sistema de Pagos.

Para las Entidades:

- Preparar sus oficinas para implementar procesos de registro y entrega de Certificados Digitales de acuerdo a las políticas definidas por la Dirección de Certificados de Firma Digital.

- Concentrar sus esfuerzos y recursos en el diseño y puesta en marcha de Sitios Web que utilicen los certificados brindados por el Sector Financiero.

- Llevar adelante los trabajos de reingeniería de procesos para atender los requerimientos de los servicios financieros por Internet.

CONCLUSIONES

La seguridad informática es un aspecto que con el paso del tiempo recobra mayor importancia para las organizaciones. La tecnología es un aliado de los negocios, simplificando y automatizando procesos. Es necesario realizar una modernización que haga más eficiente y eficaz la prestación de servicios, donde se rompa los paradigmas que por años han sido sujetos gran cantidad de instituciones del estado nacional.

La modernización de procesos conlleva un exhaustivo trabajo de formación, en donde se deja de lado el nivel de comunicación jerárquico utilizado a través de los años, impregnado de burocracia y largas gestiones administrativas y se adopta un sistema horizontal de múltiples vías, que facilita en gran medida y agiliza las actividades.

Es un proceso lento pero eficaz siempre y cuando se definan adecuadamente los procedimientos, no solamente se requiere brindar los servicios, estos deben estar sujetos a una innovación continua, acorde a demandas nacionales e internacionales.

A nivel nacional se requiere de fuertes inversiones en materia de seguridad informática, que garantice la continuidad de las operaciones y el eficiente manejo de las mismas, la definición de políticas que velen por la seguridad de la información ha sido un esfuerzo respetable para nuestras autoridades gubernamentales, pero se requiere de mayores esfuerzos para difundir esas políticas y directrices.

Es necesario un cambio de actitud, iniciando por las altas autoridades del estado, se requiere de una nueva cultura política y social, para que la ciudadanía costarricense forme parte de ese cambio, adaptándose al entorno tecnológico, lo cual le brinda al país la oportunidad de implantar su modelo de gestión de seguridad, acorde a las necesidades existentes.

BIBLIOGRAFÍA

Cisco Systems (2004). *Guía del primer año CCNA 1 y 2*. Madrid: McGraw-Hill.

Cisco Systems (2004*). Guía del segundo año CCNA 3 y 4*. Madrid: McGraw-Hill.

ISACA (2000). *Information Systems Audit and Control Association*. Madrid: Borrmart

Academia Latinoamericana de Seguridad Informática (2007). *Introducción a la seguridad de la información*. Recuperado el 8 de febrero del 2009, de h*ttp://www.terra.es/tecnologia/articulo/html/tec9481.htm.*

Cisco (2007). *Cisco integra Nac en sus routers de servicios integrados*. Recuperado el 18 de febrero del 2009, de www.cisco.com.

ISO (2006). *Estándares de seguridad informática. ISO 17799*. Recuperado el 25 de febrero del 2009, de www.iso.com.

Firewalls (2008). *Firewalls para aplicaciones empresariales*. Recuperado el 2 de marzo del 2009, de http://www.aplicacionesempresariales.com/files/2008.

IDS (2007). Sistema de detección de intrusos. Recuperado el 12 de Marzo del 2009, de http://www.uv.es/montanan/redes/trabajos/IDSs.ppt#274,19

Mricrosoft (2006). Internet Security acceleration Server. Recuperado el 14 de Marzo del 2009, de www.microsoft.com.

MICIT (2009). *Encuesta realizada por el Ministerio de Ciencia y tecnología de Costa Rica.* Recuperado el 18, de www.micit.com.

Gobierno digital (2008). *Resumen ejecutivo*. Recuperado el 20, de http://www.gobiernodigital.org/Que-es-un-Gobierno-Digital