(Tipo./Ing./Esp./MSc./PhD.)

Nombre(s)

Octubre.2000

# ESCUELA POLITÉCNICA NACIONAL

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

# ANÁLISIS Y DISEÑO DE UNA ESTRUCTURA DE SEGURIDAD INFORMÁTICA EMPLEANDO COBIT PARA ANDINATEL S.A.

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN**

**CHRISTIAN ANÍBAL ROMERO ZÁRATE**

**cromero_z@msn.com**

**DIRECTOR: ING. TARQUINO SÁNCHEZ ALMEIDA**

**tarquino.sanchez@epn.edu.ec**

**Quito, marzo 2010**

# DECLARACIÓN

Yo Christian Aníbal Romero Zárate, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

**Christian Romero**

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Christian Aníbal Romero Zárate, bajo mi supervisión.

_____

Ing. Tarquino Sánchez
DIRECTOR DEL PROYECTO

## DEDICATORIA

A mis padres, esposa y hermano por su apoyo incondicional
y siempre sincero, los amo mucho.

## CONTENIDO

# RESUMEN

El presente trabajo se enmarca en el mejoramiento del proceso de seguridad en la Corporación Nacional de Telecomunicaciones (CNT, anteriormente conocida como Andinatel S.A.) mediante el desarrollo de una estructura de seguridad informática utilizando el CoBIT como marco de referencia. Esta estructura de seguridad informática es un conjunto de políticas, procedimientos y soluciones de seguridad.

Se determina en primera instancia el nivel de seguridad que en el momento del desarrollo del presente trabajo, posee la CNT. En base a la información recabada por la auditoria al proceso DS5 de CoBIT dentro de la institución, y enmarcada dentro de la Gerencia de TI (ex Vicepresidencia de Sistemas). La categorización de este nivel nos permitirá determinar cuánto debemos mejorar en el proceso de seguridad y el alcance de las políticas, procedimientos y soluciones de seguridad informática propuestas. Con estos datos e información podemos realizar un análisis de costos que nos permitirá determinar la viabilidad de la implementación de los proyectos propuestos en este trabajo.

En el capítulo 1 se describirá brevemente el desarrollo de las telecomunicaciones en el mundo haciendo una comparación con lo sucedido en el Ecuador para luego particularizar en el caso de la Corporación Nacional de Telecomunicaciones. Se expondrán los estándares de seguridad de la ISO, así como recopilaciones de buenas prácticas como ITIL para luego centrarnos en CoBIT. Analizaremos las principales amenazas que las empresas actualmente poseen. A continuación en el capítulo 2 realizaremos la auditoria al proceso de seguridad y en el capítulo 3 estableceremos, en base al nivel de madurez encontrado, las acciones a seguir para mejorar el nivel de seguridad. Con esta información en el capítulo 4 veremos el costo de implementación de lo propuesto en el capítulo 3, y terminaremos en el capítulo 5 con las conclusiones y recomendaciones del presente trabajo.

# PRESENTACIÓN

La información se ha vuelto, en estos últimos años, en el activo más importante para la supervivencia de las empresas en el competitivo mundo actual, mucho más cuando sus operaciones están basadas en tecnología. Esta necesidad de información ha forzado a que las instituciones tomen medidas para precautelar su integridad, disponibilidad y confidencialidad, manejando esquemas de respaldos, controles de acceso y contingencias; sin embargo estas medidas podrían dar o no los resultados deseados en un tiempo determinado. Los estándares y "buenas practicas" ayudan a las organizaciones a dirigir sus esfuerzos en pos de mejorar el ambiente de control y la administración de las tecnologías de la información, en este contexto y para el caso de la seguridad informática existen los estándares ISO/IEC 17799, 2700x, además de buenas prácticas como el CoBIT e ITIL.

CoBIT nace justamente de la necesidad de alinear los objetivos de TI con los objetivos organizacionales implementando para tal efecto una serie de controles para cada proceso de tecnología, para nuestro caso el proceso DS5 denominado "Garantizar la seguridad de los sistemas", en donde se resume una serie de sugerencias para obtener un resultado deseado: un manejo de información que le permita a la empresa alcanzar objetivos mediante un manejo adecuado de los riesgos tecnológicos.

Mediante la auditoria a los procesos siguiendo el marco referencial de CoBIT podemos establecer brechas que permitirán mejorar los procesos hasta un nivel deseado, mediante el establecimiento de directrices que se traducen en planes de acción. De esta manera los procesos de TI y el crecimiento de las tecnologías de la información así como su administración es mejorada y controlada, ya que permite establecer controles que minimizan riesgos para la consecución de objetivos o metas organizacionales. El éxito de la organización depende en gran medida de que se entienden los riesgos y se aprovechan los beneficios de las tecnologías de la información.

# CAPÍTULO 1

## 1.1. INTRODUCCIÓN

En el presente capitulo se realizará una reseña histórica de las telecomunicaciones en el mundo y como éstas se desarrollaron en el Ecuador. Revisaremos como se conformaron las empresas de telecomunicaciones en el país hasta convertirse en la actualidad en una sola: la Corporación Nacional de Telecomunicaciones. Revisaremos como las empresas que basan sus procesos de negocio en tecnología sufren de incidentes relacionados con la seguridad informática, y revisaremos como las empresas hacen frente a esta problemática mediante la implementación de procesos relacionados con el manejo y administración de tecnología y seguridad.

## 1.2. LAS TELECOMUNICACIONES Y SUS INICIOS

Ya han pasado más de 177 años cuando Paul von Schilling en 1832 recogió las experiencias de varios científicos para producir el telégrafo electroquímico que enviaba mensajes entre varias estaciones de tren, la eficiencia en ese entonces suponía una velocidad de transmisión superior a la velocidad de los trenes que en aquella época bordeaba los 45Km/h para que la comunicación tenga algún sentido. Un año más tarde Wilhelm Weber y Carl Frederich Gauss construyen el telégrafo con aguja electromagnética y logran comunicar a la Universidad de Gatinga con el Observatorio Astronómico ubicado en la misma ciudad. Los mensajes eran enviados y recibidos de acuerdo al movimiento de la aguja, el cual era producido por una bobina a la cual se la exponía a cambios de corriente eléctrica.

El salto más importante en la historia de la telegrafía lo da un pintor, Samuel Finley Morse. En sus viajes por Europa conoció los primeros telégrafos y en el viaje de regreso, a través del Atlántico, diseñó un sistema de transmisión a través de un código que reducía de manera significativa la cantidad de signos y letras que se transmitían a través de los medios de comunicación telegráfica aumentando así su eficiencia. Esta clara intuición semántica basada en puntos y rayas (vibraciones cortas y largas) que se trasmitían en un solo alambre, permitió

que el 24 de mayo de 1844 (exactamente 12 años después de la batalla de pichincha para ponernos en un contexto histórico nacional), transmitir el primer mensaje que decía “lo que Dios ha hecho” recibido en Baltimore y enviado desde Washington en los Estados Unidos de Norteamérica.

En una especie de Internet primigenia, la red telegráfica se expandió en todo el territorio Norte Americano desde el año 1845. 6 años más tarde en Inglaterra se tendió el primer cable submarino para unir los puertos de Dover y Calais ubicado en Francia. Con toda la experiencia acumulada en cuanto al aislamiento de los cables, su reforzamiento y el debilitamiento de las señales experimentado en esta primera instalación, en 1858 gracias a la ayuda de los buques Agamemnón y Niágara, se tendió el primer cable trasatlántico telegráfico en una distancia de 3240 Km. [1]

En América del Norte por su parte se instalo el primer cable intercontinental uniendo Cuba y la Florida en el año 1867 trabajo realizado por parte de la empresa Central and South American Cable Company[2]; la misma que 4 años más tarde instalaría la primera línea telegráfica en el Ecuador.

El 4 de julio de 1876, luego de 5 meses de la polémica de patentes, Alexander Graham Bell presentó su invento con la presencia de pocas personas. Luego de ganar el derecho de explotar su invento fundó la empresa Bell Telephone Company que para 1891 controlaba más de 240.000 teléfonos[3]. Esta tecnología permitía la conexión punto a punto, es decir, se tenía que instalar tantas líneas como puntos de comunicación se querían tener. La primera central telefónica comenzó a operar en 1878 en New Haven (cuando estábamos en el Ecuador

[1] Datos históricos tomados de la página del profesor Luis Enrique Otero Carvajal, Profesor Titular de Historia Contemporánea. Universidad Complutense. Madrid. España “EL TELÉGRAFO ELÉCTRICO”, http://www.ucm.es/info/hcontemp/leoc/telegrafo%20electrico.htm

[2] Empresa fundada por James Scrymser en el año1881, para el año 1920 el nombre de la empresa fue cambiado a All American Cables.

[3] Tomado de AT&T Corp history, http://ecommerce.hostip.info/pages/59/AT-T-Corp-EARLY-HISTORY.html

montando la red telegráfica), sirviendo a 21 abonados y con 8 líneas individuales es decir se compartía el canal en una proporción aproximada de 3 a 1. [4]

Las conversaciones en este esquema sufrían de falta de confidencialidad ya que eran susceptibles a que los operadores puedan escucharlas, además de la lentitud de los mismos en atender y enrutar las llamadas a su destinatario cuando tenían un gran flujo de trabajo. A partir de esta situación se inventó un sistema de conmutación que ya no tenía la intervención de los operadores sino más bien era activado por los abonados.

En el año 1889 Almon Strowger propietario de una funeraria en Kansas, Estados Unidos, debido a que las llamadas eran desviadas a su competencia cada vez que se solicitaba algún servicio funerario por medio de las líneas telefónicas, decidió inventar un método bajo el cual el direccionamiento de las llamadas no dependiera de las operadoras telefónicas. El sistema se basaba en discos que hacían la vez de interruptor y dirigían la llamada hacia su destino, este sistema entro en funcionamiento en Estados Unidos en el año de 1893. Para el año de 1910, 132 poblaciones contaban con el servicio automático de conmutación telefónica dando servicio a más de 200.000 abonados[5]. En el Ecuador la historia de la telegrafía y telefonía empezó a escribirse con el gobierno de Gabriel García Moreno.

### 1.2.1. LAS TELECOMUNICACIONES EN EL ECUADOR

Gabriel García Moreno en su segundo periodo Presidencial 1869-1875 decide impulsar el proyecto de comunicación telegráfica en el país mediante 2 ejes primordiales las comunicaciones a través de la instalación del telégrafo, y a través del ferrocarril. En 1873 comienza la construcción de las rieles entre Quito y Guayaquil, la idea para la transmisión de mensajes telegráficos constituía en

[4] Tomado de la página web de la AHCIET, Asociación Iberoamericana de Centros de Investigación y Empresas de Telecomunicaciones, http://www.ahciet.net/historia/pais.aspx?id=10150&ids=10682.
[5] Tomado de http://worldoffice.wordpress.com/2009/12/30/voz-datos-y-calor/

instalar paralelamente a las líneas férreas los cables telegráficos. En el año de 1875 funcionó por primera vez el telégrafo entre Yaguachi y Milagro en una distancia comprendida por 44.6 Km. La muerte de Gabriel García Moreno retrasaría la Obras de construcción de este proyecto.[6]

El telégrafo que se instalaba en ese entonces en el Ecuador no poseía las capacidades de transmisión que había impuesto el código Morse, más bien se trataba de un modelo que ya había dejado de usarse en otras partes del mundo y se basaba en la identificación de letras o cifras por medio del movimiento electromagnético de una aguja, se usaba además 2 cables para la transmisión una para el mensaje de ida y otra para el mensaje de vuelta.

En el periodo presidencial comprendido entre 1876 y 1883, el general Ignacio Veintimilla continúo con el proyecto y en 1882 ya se había llegado hasta puente de Chimbo, además se sustituyo el sistema antiguo por el sistema de Morse y la utilización de un solo cable para la transmisión con el retorno de la corriente por tierra y se trabajo en la comunicación con el mundo por medio del tendido de cable entre Salinas y Panamá por medio de la misma empresa. En el año 1884 ya se había transmitido el primer mensaje entre Quito y Guayaquil, al mismo tiempo que gracias a las conexiones internacionales ya instaladas el presidente Caamaño pudo enviar un mensaje al presidente de los Estados Unidos, Chile y Perú.

Luego de la construcción de estas redes telegráficas surgió una gran interrogante ¿Quién operaria los equipos? En ese entonces no existía el personal calificado para manipular la nueva tecnología implementada, es por esta razón que el primer grupo de personas con las habilidades y conocimiento que operaron el telégrafo en el Ecuador fueron 3 peruanos y 1 cubano.

[6] Tomado del "Compendio histórico de las telecomunicaciones en el Ecuador" elaborado por la Superintendencia de Telecomunicaciones en agosto de 2007.

Si bien el telégrafo para el 1892 contaba ya con una red de alrededor de 15 mil kilómetros montados sobre el territorio ecuatoriano los mensajes no podían ser distribuidos para la mayoría de los ecuatorianos ya que los mensajes eran transmitidos y recibidos en las oficinas donde se disponía de los equipos de transmisión y recepción. Esto contribuyó a que en 1920 se creará una nueva profesión la de "Mensajeros Ciclistas" que suponía que entre 15 y veinte minutos, luego de recibido el mensaje, este sería entregado a su destino.

En el Ecuador la primera central telefónica se instaló en el año 1900, y en el año 1904 el presidente Leonidas Plaza Gutiérrez dicta un reglamento provisional para la instalación de líneas privadas. El 9 de Octubre de ese mismo año entró en funcionamiento la Compañía Nacional de Teléfonos en Guayaquil con 400 abonados y el 17 de noviembre de 1915 se implementó la primera planta telefónica en Quito. Gracias a un acuerdo con la empresa Telegráfica "The Guayaquil and Quito Railway Co." se pudo realizar llamadas de larga distancia a todas las ciudades que estaban en los alrededores de las líneas férreas[7].

Un nuevo sistema traído por la empresa Ericsson se implementó en Quito hacia el año 1927, para lo cual se construyó el Palacio de las Telecomunicaciones, actualmente donde se ocupa la Vicepresidencia de la República. El sistema de conmutación automático fue implementado en la ciudad de Quito y Guayaquil gracias nuevamente a la empresa Ericsson en el año de 1947. 2 años más tarde se creó la Empresa de Teléfonos Quito, para administrar el sistema automático. En Guayaquil la empresa se llamó Empresa de Teléfonos Guayaquil el servicio se inicio formalmente en el año 1955 con 2300 abonados.[8]

El mundo de las telecomunicaciones tuvo un gran salto debido al desarrollo de la transmisión Satelital, que mediante satélites ubicados en orbitas geoestacionarias

[7] Tomado del "Compendio histórico de las telecomunicaciones en el Ecuador" elaborado por la Superintendencia de Telecomunicaciones en agosto de 2007.
[8] Tomado del "Compendio histórico de las telecomunicaciones en el Ecuador" elaborado por la Superintendencia de Telecomunicaciones en agosto de 2007.

permitían la comunicación en diferentes partes del mundo. Un proceso que fue iniciado por la Unión Soviética de ese entonces, en los inicios de la guerra fría por medio de la fabricación del Sputnik 1, pequeño artefacto de 80 Kg. que orbitaba entre 200 y 900 Km. emitiendo señales de radio y desintegrado al intentar ingresar a la atmósfera el 3 de enero 1958.

En febrero de 1971 se dicta una ley mediante la cual se crean dos empresas adscritas al Ministerio de Obras Públicas y Comunicaciones: la Empresa de Telecomunicaciones del Norte, con jurisdicción en las provincias de Esmeraldas, Carchi, Imbabura, Pichincha, Cotopaxi, Tungurahua, Chimborazo, Bolívar, Napo y Pastaza y la Empresa de Telecomunicaciones del Sur, con jurisdicción en las provincias de Manabí, Los Ríos, Guayos, El Oro, Cañar, Azuay, Loja, Morona Santiago y Zamora Chinchipe.

No sería hasta el 19 de octubre de 1972 que se instala la primera estación terrena en Guangopolo al sur de Quito, una antena de 30 metros de diámetro y 300 toneladas de peso, previo concurso de licitación convocada por las empresas de telecomunicaciones del Norte y del Sur en donde se solicito además red nacional de microondas y una red nacional de Telex gentex. [9]

El 16 de octubre de 1972 el Gobierno Nacional, mediante Decreto Supremo crea el Instituto Ecuatoriano de Telecomunicaciones (IETEL) resultado de la fusión de las empresas de telecomunicaciones del Norte y del Sur y la Dirección Nacional de Frecuencias. El IETEL se creó con la finalidad de planificar, desarrollar, establecer, explotar, mantener, controlar y regular todos los sistemas de telecomunicaciones nacionales e internacionales, exceptuando únicamente los de las Fuerzas Armadas y la Policía.

En ese entonces se tenían los siguientes servicios:

[9] Tomado del "Compendio histórico de las telecomunicaciones en el Ecuador" elaborado por la Superintendencia de Telecomunicaciones en agosto de 2007.

### Telefonía Local

El Ecuador a diciembre de 1972, disponía de 128,000 líneas de central (LC), 123.000 a cargo del IETEL y 5.000 de ETAPA. Un total de 120.542 (LP) líneas principales en servicio para 6.432.199 habitantes daban como resultado una densidad telefónica de 1,87 LP por cada 100 habitantes.

Durante el período 1973 a 1979 se instalaron 129.750 LC, con lo cual el país a diciembre de 1979 disponía de 257.750 LC y 213.972 LP, obteniéndose una densidad telefónica de 2,7. Del total de líneas de central, el 36,8% se concentraba en Quito, el 38,4% en Guayaquil, el 3,8% en Cuenca y el 22% en diferentes áreas del país.

En el período de 1980 1984 no se instalaron nuevas centrales, sino que se utilizó en forma inadecuada la capacidad instalada llegando a superar el 94% de ocupación, lo que ocasionó problemas técnicos y administrativos. Al finalizar el se alcanzó una densidad de 3,03%.

De 1985 a 1989 se reinició la instalación de nuevas centrales, lo que permitió incrementar la tasa de crecimiento anual y el país tenía una densidad de 4,2%. Durante 1990 la densidad telefónica alcanzó un valor de 4,4%.

### Telefonía de Larga Distancia Nacional

En 1979 el tráfico de larga distancia se cursaba mediante las centrales de tránsito instaladas una en Quito, con una capacidad de 2.000 terminales, y otra en Guayaquil, con una capacidad instalada de 1.600. La capacidad de las centrales de tránsito no eran suficientes para cursar el tráfico telefónico de larga distancia, lo que producía una alta congestión y, en consecuencia, una gran cantidad de llamadas se perdían. Esto obligo que durante el período 1980 1984 se incrementaron las capacidades de las centrales de tránsito y pasos de larga distancia en 2.400 terminales, con lo cual se contaba al final del período con 6.000 terminales.

En el período 1985 1989 se instalaron nuevas centrales de tránsito digitales en Quito, Guayaquil y Cuenca, con una capacidad al final del período de 11.370, 13.300 y 2.048 terminales respectivamente.

**Telefonía Internacional**

En 1974 se puso en servicio la central de tránsito internacional con una capacidad de 200 terminales. En el período de 1975-1980 se incrementó esta central a 800 terminales. Esta capacidad se mantuvo en el período 1980 1984 y entre 1985 a 1989 se incrementó a 1.000 terminales.

En 1971 el Ecuador es aceptado como miembro de INTELSAT y un año más tarde se integra a las comunicaciones vía satélite, cuando entró en servicio la Estación Terrena instalada en Quito, con una capacidad inicial de 36 circuitos, de los cuales se utilizaban 24.

La demanda del servicio telefónico internacional se incrementó rápidamente siendo necesaria en 1976 la ampliación de 120 circuitos y en 1978 a 156 circuitos. A diciembre de 1979 se encontraban en servicio 135 circuitos, de los cuales 122 eran para telefonía y 13 para datos y telegrafía. A diciembre de 1984 se disponía de 284 circuitos y de un equipo para transmitir señales de televisión hacia el satélite y a diciembre de 1989 de 390 circuitos.

En el período 1980 1984 se tomó la decisión de iniciar en forma sistemática la adquisición de centrales de tecnología digital. Se contrataron 73.500 líneas de centrales locales digitales para las ciudades de Quito, Guayaquil y la provincia de Bolívar, para cuyo funcionamiento se contrató también aproximadamente 18.000 líneas de central de tránsito digital para las ciudades de Quito, Guayaquil y Cuenca.

En 1988 y 1989 se ampliaron algunas centrales digitales y se instalaron nuevas centrales de la misma tecnología en otras ciudades del país, alcanzándose un porcentaje de digitalización del 43%. ETAPA, explotadora del servicio telefónico en la ciudad de Cuenca inició la digitalización de su red en el año 1987. Las ciudades de Quito, Guayaquil y Cuenca disponían de redes digitales superpuestas a las analógicas que serán absorbidas en los próximos años.

La Ley Especial de Telecomunicaciones, publicada en el Registro Oficial 996 de 10 de agosto de 1992 crea la Empresa Estatal de Telecomunicaciones (EMETEL) y la SUPTEL, en sustitución del Instituto Ecuatoriano de Telecomunicaciones (IETEL), organismo público que cumplía el doble papel de operador y regulador. Posteriormente, la Ley Reformatoria del 30 de agosto de 1995, llevó a cabo una reestructuración en el sector con la delegación de la explotación de los servicios en el sector privado, y estableciendo como instrumento de tal proceder la transformación de Emetel con la posterior venta parcial de paquetes accionarios. Esta Ley también creó el Consejo Nacional de Telecomunicaciones (CONATEL), para ejercer las funciones de administración y regulación de los servicios de tele comunicaciones en el país. Decretando igualmente la creación de la Secretaría Nacional de Telecomunicaciones (S.N.T.), que tiene, entre otras, las funciones de cumplir y hacer cumplir las resoluciones del CONATEL, así como ejercer la gestión y administración del espectro radioeléctrico.

En ejecución del plan legal, Emetel se transformó en EMETEL S.A., y, posteriormente, el 18 de noviembre de 1997, se escindió en dos compañías regionales, ANDINATEL y PACIFICTEL. Una vez concluida la segregación se había programado realizar una subasta del 35% de las acciones de cada una de las compañías resultantes de la misma. Pasarían 11 años para que estas 2 nuevas empresas vuelvan a unirse en una única empresa denominada Corporación Nacional de Telecomunicaciones S.A.

La Corporación Nacional de Telecomunicaciones se creó mediante escritura pública, el 1 de Octubre de 2008, y fue aprobada mediante Resolución 08.Q.IJ.4458 emitida por la Superintendencia de Compañías. En la actualidad la CNT S.A. abarca el 90% del mercado de telefónica fija, la siguiente la Fig 1.1 nos muestra las estadísticas actuales de distribución de abonados:

Telefonía Fija, de un total de 1´979.991 usuarios:

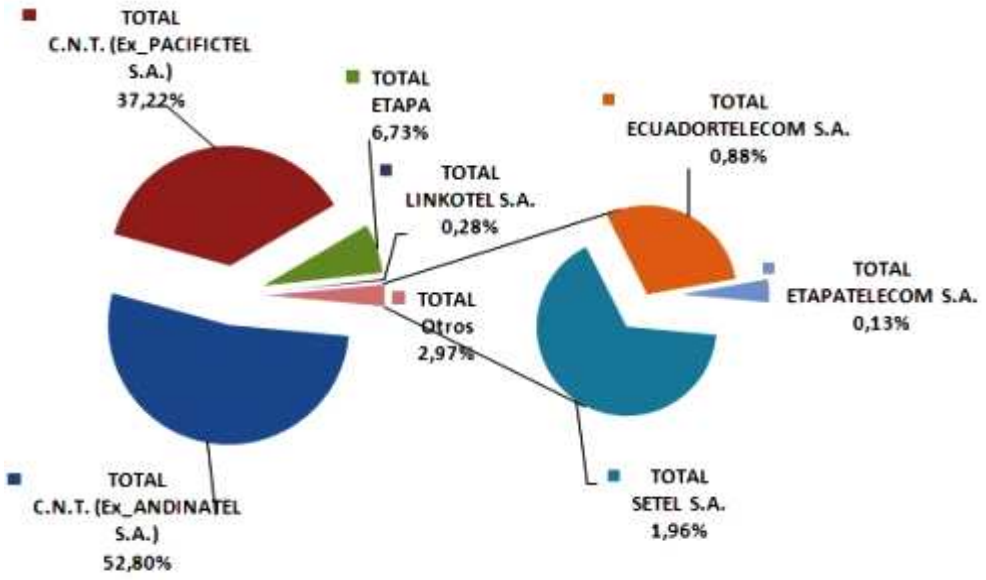



Fig 1.1 Abonados en la telefonía fija

El 28 de Octubre de 20087 el Presidente de la República, Rafael Correa, firmó el decreto mediante el cual se crea el nuevo Ministerio de Telecomunicaciones y de la Sociedad de la Información. Esta nueva cartera de Estado se encargará de la formulación de políticas públicas en materia de información; así como de la coordinación de las instituciones públicas y privadas en materia de investigación científica y tecnológica. El secretario Jurídico de la Presidencia, Alexis Mera, adelanta además que se fusionará el Consejo Nacional de Radio y Telecomunicación, (Conartel) con el Consejo Nacional de Telecomunicaciones (Conatel). Asimismo, las funciones administrativas que ejercía el presidente del Conartel ahora serán ejecutadas por la Secretaría Nacional de Telecomunicaciones (SENATEL).Parte de las competencias de este ministerio es

promocionar el uso del Internet y de las tecnologías de la información. Además de hacer un seguimiento y supervisión de las empresas del Estado dedicadas a telecomunicaciones y tecnologías de información. [10]

Aunque las modificaciones realizadas hasta el momento habían permitido la transformación del modelo de telecomunicaciones, el Gobierno de Gustavo Noboa decidió, en marzo de 2000, reformar de manera sustancial la Ley de Telecomunicaciones al abrir, de acuerdo a la Ley Para la Transformación Económica, todos los servicios a la libre competencia. Esta apertura del mercado fue fijada para el 1 de enero de 2002.

El 2 de enero de 2002, se hizo oficial la Apertura del Mercado de las Telecomunicaciones, que inicia la libre competencia con el proceso de subasta de las redes de acceso inalámbrico de tecnología Wireless Local Loop (WLL).

**Telefonía Celular**

A finales de 1993, se inicia el servicio de telefonía celular en el país con la entrada en el mercado de Conecel S.A. (Porta Cellular) y Otecel S.A. (actualmente Movistar).

Aunque el 2 de agosto de 1993 se formalizó la asignación de la banda A a Conecel S.A. (Porta Cellular), no fue sino hasta diciembre cuando el presidente de la República del Ecuador, Sixto Durán Ballén, realiza la primera llamada oficial desde Conecel S.A. (nombre de la razón social de la compañía) en Guayaquil.

[10] Nota del Universo, del martes 28 de octubre de 2008, "Fusión telefónica crea la nueva CNT" Noticias - Políticas y planes de acción

Ya en 1994, Conecel, más conocida por su nombre comercial “Porta”, supera sus expectativas de obtener 2.000 abonados en Quito y 3.000 en Guayaquil, llegando a 14.000 a finales de año. En 1996 esa cifra se eleva a 33.000, y a 50.000 en diciembre de 1997. [11]

En julio de 1998, la operadora empieza a ofrecer servicios de Internet, mientras que en marzo de 2000, Telmex, empresa líder en telecomunicaciones de Latinoamérica y una de las principales empresas mundiales, adquiere el 60% de la participación accionarial de Conecel, impulsando un agresivo programa de inversiones dirigido a ampliar la cobertura y modernizar la red de Porta.

El 24 de agosto de 1998, se publica la Resolución de Conatel No. 421-27, en la cual se aprueba el Reglamento para el Servicio de Telefonía Móvil Celular, principal competencia para el servicio de telefonía fija.

En septiembre de ese año, Porta pasa a depender de la mexicana América Móvil, filial de Telmex, lo que le permite alcanzar los 405.000 usuarios en 2001, consolidando su posición en el mercado ecuatoriano.

Por su parte, Otecel S.A. inició operaciones en la banda B, en enero de 1994, utilizando tecnología TDMA suministrada por Ericsson. La adquisición de su mayoría accionarial por Bellsouth en marzo de 1997 le permitió aumentar sus abonados en casi un 100% en tan solo un año (período 1997-1998).

La figura 1.2 muestra la distribución de los principales operadores del país, con relación a 12´352.000 usuarios entre abonados postpago y prepago, a principios de 2010:

[11] Tomado de la página web oficial de la SUPERTEL, Superintendencia de Telecomunicaciones del Ecuador.

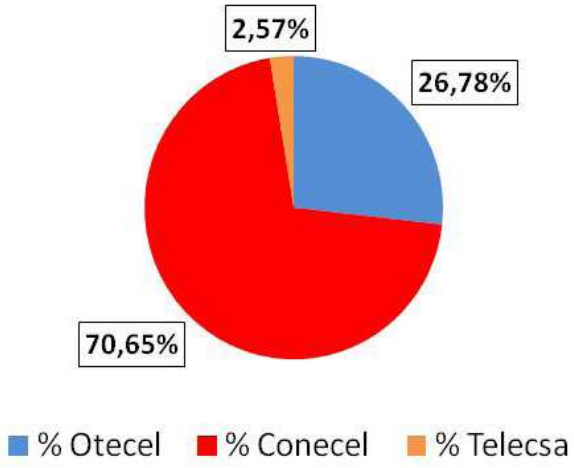



Fig 1.2 Abonados en la telefonía celular

Este rápido crecimiento de los servicios de Internet, telefonía móvil y telefónica fija a obligado a las empresas del Ecuador a invertir fuertes cantidades de dinero en busca de acaparar el mercado. La telefonía fija ha tenido a lo largo del tiempo un solo proveedor del servicio a manos del estado, mientras que la telefonía móvil o celular ha tenido la participación extrajera resumida en 2 grandes empresas que acaparan más del 95% del mercado ecuatoriano.

## 1.3. SEGURIDAD DE LA INFORMACIÓN

Todas las empresas señaladas con anterioridad poseen algo en común, sus operaciones basan su accionar en tecnología, se apoyan en ella y de ella dependen para alcanzar sus objetivos estratégicos. Debe existir entonces una completa sinergia entre los objetivos de una empresa y la tecnología que la soporta. La información y la tecnología relacionada son los activos más valiosos de las empresas, transformándose así en un elemento crítico para el éxito y la supervivencia de las organizaciones, dependiendo necesariamente de una administración efectiva de las tecnologías de la información.

La información es uno de los activos más importantes que tiene una empresa así como el recurso humano o el capital. Cada uno de estos activos es administrado ya sea por una área de recursos humanos, por departamentos financieros. Pero la información, y no hasta hace mucho, ha sido relegada de su importancia como factor crítico para la supervivencia de las organizaciones y el cuidar de este activo se vuelve más importante y necesario así como su gestión y continuo mejoramiento.

Hay numerosos cambios en el entorno de TI y en su ambiente de operación que enfatiza la necesidad de un mejor manejo de los riesgos tecnológicos. La dependencia de la información electrónica y los sistemas de TI son esenciales para soportar los procesos críticos del negocio. Adicionalmente, el ambiente regulatorio demanda control estricto sobre la información. Esto a su vez conduce a un incremento de los desastres en los sistemas de información y al incremento del fraude electrónico. Por lo tanto se ve la necesidad de protección de los activos de información.

El advenimiento del intercambio electrónico a través de los proveedores de Internet y directamente con los clientes, la pérdida de barreras organizacionales a través de herramientas remotas y la exposición a riesgos de seguridad de alto impacto tales como virus, ataques de denegación de servicio, intrusiones, acceso no autorizado, revelación y robo de números de tarjetas de crédito a través de Internet han elevado el perfil de riesgo de la información y de la privacidad y con esto la necesidad de gestionar con eficacia la seguridad de la información.

La seguridad de la información se basa en tres pilares fundamentales:

a) **Confidencialidad.**- Protección de la información sensible contra divulgación no autorizada,

b) **Integridad.-** Precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

c) **Disponibilidad.**- La información disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.[12]

Dentro de estos preceptos se han enmarcado algunos de los más importantes métodos y metodologías relacionadas con la seguridad de la información y de los cuales nos referiremos a continuación:

-ESTÁNDARES ISO DE SEGURIDAD

-ITIL

-COBIT

### 1.3.1. ESTÁNDARES ISO DE SEGURIDAD

Uno de los primeros estándares en recopilar una serie de buenas prácticas en relación a la seguridad de la información son las normas BS7799[13] que luego tomaron el nombre de ISO/IEC 17799. En esta norma existe una nuevas definiciones con relación a lo que expone CoBIT con respecto a la confidencialidad integridad y disponibilidad de la información:

a) **Confidencialidad.-** Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

b) **Integridad.-** Garantía de la exactitud y el contenido completo de la información y los métodos de su procesamiento.

c) **Disponibilidad**.- Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados,[14]

[12] Conceptos tomados del Marco de Referencia CoBIT, del IT Governance Institute 3ra edición
[13] Por sus siglas en ingles British Stándard. Fue creado por el British Standard Institute en el año de 1995.
[14] Tomado de la norma ISO/IEC 17799:2005, creado por la organización Internacional para la Estandarización/Normalización

La norma 17799:2005 recopila 127 objetivos de control divididos en 11 áreas que detallo a continuación:

| Dominios | Descripción de los dominios de la norma 17799:2005 |
|---|---|
| Política de seguridad | Dirigir y dar soporte a la gestión de la seguridad de la información. |
| Aspectos organizativos de la seguridad | Gestionar la seguridad de la información dentro de la organización. |
| Administración de activos | Mantener una protección adecuada sobre los activos de la organización. |
| Seguridad ligado al personal | Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. |
| Seguridad física y ambiental | Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. |
| Gestión de comunicaciones y operaciones | Asegurar la operación correcta y segura de los recursos de tratamiento de información. |
| Control de accesos: | Controlar los accesos a la información. |
| Desarrollo y mantenimiento de sistemas | Asegurar que la seguridad esté imbuida dentro de los sistemas de información. |
| Gestión de continuidad del negocio | Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres. |
| Administración de los incidentes de seguridad de la información | Asegurar una correcta administración de los incidentes de seguridad, reporte manejo y cierre. |
| Cumplimiento | Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad. |

Tabla 1.1, descripción de los dominios de la norma de seguridad ISO/IEC 17799:2005

Esta norma no es certificable pero brindaba un buen comienzo acerca de los controles a implementar en una organización que busca proteger sus activos de información.

En el año 2005 este mismo organismo remitió los estándares certificables para las empresas a los estándares de calidad ISO 9000, en cuanto a la certificación y su

forma de obtenerla, a estos se los denominaría estándares ISO 27000 que en su esencia poseen los mismos controles que la norma 17799. A continuación una breve explicación:

| Normas ISO 2700X | Componente principal | Nombre |
|---|---|---|
| ISO/IEC 27001 | BS7799-2 | Sistema de Administración de la Seguridad de la Información |
| ISO/IEC 27002 | ISO/IEC 17799 &BS7799-1 | Código de Práctica |
| ISO/IEC 27003 | BS7799-3 | Análisis de Riesgos |
| ISO/IEC 27004 | BS7799-4 | Métricas y medidas para la seguridad de la información |

Tabla 1.2, enumeración de las normas 2700X

Así como las certificaciones ISO de calidad, las de seguridad se obtienen pasando un checklist donde se enumeran los controles que dicta la norma. Al final de la revisión se tiene una lista de controles faltantes para poder ser certificados, las recomendaciones basan su criterio en la implementación del control faltante siguiendo las directrices dictaminadas en el estándar.

### 1.3.2. ITIL

Creado a finales de la década de los 80´s por la empresa CCTA (Central Computer And Telecommunication Agency, por sus siglas en ingles), del Reino Unido luego de que el proyecto TAURUS II auspiciado por el gobierno de ese entonces fracasará gastando alrededor de 20 millones de dólares[15], su objetivo principal crear una metodología para gestionar los procesos de tecnologías de la información. En la actualidad está regulado y patentado por el Ministerio de Comercio (OCG, antes denominado CCTA) del Reino Unido. Se puede resumir el desarrollo de ITIL de la siguiente manera:

[15] El proyecto Taurus ha sido bien documentado como generalmente se hace con proyectos realizados con fondos públicos, TAURUS son las siglas de TRANSFER AND AUTOMATED REGISTRATION OF UNCERTIFICATED STOCK, cuyo objetivo era la eliminación de papeles en las transacciones de la bolsa de Londres. Luego del fracaso de este proyecto el Gobierno Británico encargaría el proyecto a la CCTA para encontrar las prácticas exitosas en la gestión de servicios.

| Año | Descripción |
|---|---|
| 1986 | Inicia el desarrollo de ITIL |
| 1989 | Primeras publicaciones de ITIL versión 1[16] |
| 1991 | Fundación del grupo de usuarios |
| 2000 | Nace ITIL V2 |
| 2007 | Publicación de ITIL V3 |

Tabla 1.3, historia del desarrollo de ITIL[17]

Es una biblioteca que documenta las buenas prácticas de la gestión de servicios de TI, toda la experiencia de las empresas que han tenido éxito en la implementación de procesos de TI se encuentra condensada en esta recopilación.

Existen en la actualidad 2 versiones de ITIL que son ampliamente difundidas e implementadas la versión 2 y 3 de. La versión 2 del ITIL se encuentra resumida en 7 libros:

a) Prestación de Servicios
b) Soporte al Servicio
c) Gestión de la infraestructura de TI
d) Gestión de la seguridad
e) Perspectiva de negocio
f) Gestión de aplicaciones
g) Gestión de activos de software

La versión 3 de ITIL, por su parte posee 5 libros:

a) Estrategia del Servicio
b) Diseño del Servicio
c) Transición del servicio
d) Operación del Servicio

[16] Inicialmente denominado GITMM,Government Information Technology Infraestructure Management Metodolgy. Las letras G y M del acrónimo son eliminadas debido a que quieren ampliar su adopción. No quieren que se la vea como una metologia sino como una Guía, y no solo es gubernamental sino de alcance mundial.
[17] Tomado de la pagina http://www.itservicestrategy.com/itil-v2-itil-v3-and-iso-2000-history-and-timeline, de la empresa IT Service Estrategy.

e) Mejoramiento continuo del servicio

Pero la mayor diferencia entre las 2 versiones está en la visión del ciclo de vida que se introduce en la versión 3.[18]

ITIL en general tiene 4 pilares fundamentales:

a) Procesos: para alinear el negocio y la gestión de servicios e TI mediante la mejora constante de los procesos.

b) Calidad: basadas en los procesos y con las medidas y mejoras de los mismos, estos se alinean con normas de calidad y ayudan a la misma

c) Cliente: es beneficiario directo de la mejora de los servicios

d) Independencia: manteniendo las buenas prácticas independientes de los fabricantes marcas o tecnología.

La adopción de estas buenas prácticas no garantiza que algo funcione bien, sino que nos da una gran probabilidad de que eso ocurra. Estas adopciones de buenas prácticas por lo regular devienen en la obtención de certificaciones que avalan la adopción y la correcta implementación de las mismas, algo que a las empresas les encanta obtener para mostrarlo a sus clientes e ITIL es la excepción.

La certificación ITIL no se la obtiene directamente de la OCG, se la obtiene a través una vez más de la ISO[19] o a través de los estándares BS:

a) BS-15000 acreditada por el British Standards Institute desde el año 2000. Representa el estándar de la industria para las organizaciones que desean medir y probar sus competencias en la provisión y soporte de la gestión de servicios de TI.

[18] Tomado del articulo ITIL V2, ITIL V3 ò ISO 20000?, de Javier Garcia Arcal, Gerente de ITIL/WORKFLOW, http://www.docstoc.com/docs/8570768/%C2%BFITIL-V2-ITIL-V3-%C3%B3-ISO-20000

[19] Cuyo nombre en inglés es *International Organization for Standardization*), nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional, tomado de Wikipedia.

b) ISO-20000 Certificación en la Gestión de Servicios de TI desde el año 2005, basada en la BS 15000.

Dentro de este entorno de prestación de servicios el tema de la seguridad dentro de ITIL esta vista desde el cliente y la calidad de un servicio determinado, esto se encuentra resumido en un capítulo de la librería de ITIL denominada Gestión de la seguridad.

El capítulo Gestión de la Seguridad en resumen no se enfoca en toda la infraestructura o en la seguridad organizacional, sino en las especificaciones y requerimientos de seguridad que consten en los acuerdos, principalmente en los SLA[20]. Es así que el enfoque de ITIL es poco abarcativo dentro de este entorno sin embargo a dejado abierta las puertas para que otras buenas prácticas o estándares entren en este proceso como las ISO de seguridad o CoBIT, del cual expondré más adelante.

Ahora como determino el nivel de madurez de un proceso de ITIL pues simplemente comprando las practicas internas para la administración de TI frente a lo dictan las mejores prácticas en la industria y si estas se siguen o no, a esto se lo denomina análisis GAP. Sin embrago es de esperarse que las propias implementaciones de las empresas difieran un poco dependiendo de la realidad interna de cada organización y de su adaptabilidad a estos cambios.

### 4.2.1. COBIT

(Control Objectives for Information and related Technology | Objetivos de Control para tecnología de la información y relacionada).

[20] Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio

Creado por ISACA[21] y la ITGI[22] con la finalidad de alinear la tecnología con objetivos organizacionales. El uso de tecnología y su dependencia para alcanzar objetivos ha ido volviéndose fundamental para la supervivencia de las empresas. Las empresas necesitan de provisión eficaz de información para el desarrollo normal de sus procesos de negocio, esta información radica fundamentalmente en tecnología[23], y cada empresa tiene sus propios requerimientos de información dependiendo de su naturaleza.

¿Pero cómo satisfacer las necesidades de información de las empresas para que estas puedan cumplir con su objetivos?, o dicho de otra manera, ¿Cómo alineamos el entorno de TI a las necesidades empresariales de crecimiento y desarrollo económico?. COBIT relaciona los recursos de TI con los objetivos organizacionales proponiendo "Objetivos de Control de alto nivel" agrupados en 4 dominios, que pueden ser mapeados en cualquier organización sea cual sea su naturaleza y que requiera alineación tecnológica-objetivos organizacionales como apoyo para alcanzar sus metas empresariales. Un control por su parte son: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer aseguramiento razonable de que los objetivos del negocio serán alcanzados y de que se prevendrán o se detectarán y corregirán los eventos no deseados.

CoBIT se encuentra dividido en 4 dominios los cuales son:

- **Planeación y Organización (PO)** Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

[21] Information Systems Audit and Control Association
[22] IT Governance Institute
[23] "Más del 80% de toda la información digitalizada en una empresa reside en discos duros y dispositivos personales", The Knowledge Worker Investment Paradox"Gartner Research 07/17/2002.

- **Adquisición e Implementación (AI)** Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
- **Entrega y Soporte (DS)** En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
- **Monitoreo (M)** Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.[24]

Cada uno de estos dominios tiene su propio conjunto de objetivos de control[25] teniendo al final un total de 34.

El tema de seguridad se encuentra dentro del dominio de Entrega de Soporte (Delivery and Support, DS) en un objetivo de control de alto nivel denominado "Garantizar la Seguridad de los Sistemas" donde se encuentran además objetivos de control de bajo nivel que sirven para poder alcanzar el primero. Entre los más representativos por ejemplo se pueden encontrar:

- Manejo de las Medidas de Seguridad
- Identificación, Autenticación y Acceso
- Administración de Cuentas de Usuario
- Revisión Gerencial de Cuentas de Usuario

[24] Tomado de CoBIT 3.0

[25] Un objetivo de control se halla definido como una expresión del resultado o propósito deseado a ser alcanzado mediante la implementación de procedimientos de control en una actividad particular de TI. Los procedimientos de control son simplemente los controles establecidos para que los recursos de TI entreguen al negocio la información y el apoyo conforme a las necesidades de la empresa.

- Control de Usuario de las Cuentas de Usuario
- Vigilancia de Seguridad
- Clasificación de Datos
- Administración Centralizada de Identificación y Derechos de Acceso
- Reportes de Actividades de Violación y Seguridad
- Manejo de Incidentes
- Prevención, Detección y Corrección del Software Dañino
- Arquitectura de Firewalls y Conexiones con las Redes Públicas

El nivel de cumplimiento de lo establecido en cada uno de los objetivos de bajo nivel nos dará una medida de la madurez del proceso, que está definida en CoBIT por un puntaje que varía desde 0 hasta 5 de la siguiente manera:

**0.- Inexistente.** La organización no reconoce la necesidad de la seguridad de TI. Las responsabilidades y las obligaciones de reportar no están asignadas para asegurar la seguridad. No están implementadas medidas que soporten la administración de la seguridad de TI. No hay ningún reporte de seguridad de TI y ningún proceso de respuesta de las violaciones de seguridad de TI. Hay una carencia total de un proceso reconocible de administración de seguridad de sistemas.

**1.- Inicial /Ad hoc** La organización reconoce la necesidad de la seguridad de TI, pero la conciencia de la seguridad depende de la persona. La seguridad de TI está resuelta de manera reactiva y no se mide. Las violaciones de seguridad de TI invocan respuestas de “señalamiento” si se detectan, porque las responsabilidades no están claras. Las respuestas a las violaciones de seguridad de TI son impredecibles.

**2.- Repetible pero intuitivo** Las responsabilidades y obligaciones de la seguridad de TI están asignadas a un coordinador de seguridad de TI que no tiene autoridad de administración. La conciencia de seguridad

es fragmentada y limitada. La información de seguridad de TI es generada, pero no es analizada. Las soluciones de seguridad tienden a responder de manera reactiva a los incidentes de seguridad de TI y adoptando propuestas de terceros, sin resolver las necesidades específicas de la organización. Se están desarrollando políticas de seguridad, pero aún se siguen usando habilidades y herramientas inadecuadas. El reporte de seguridad de TI es incompleto, engañoso y no es pertinente.

**3.- Proceso definido** Existe conciencia de la seguridad y la misma es promovida por la administración. Se han estandarizado y formalizados reportes de conocimientos de la seguridad. Los procedimientos de seguridad de TI están definidos y encajan en una estructura para políticas y procedimientos de seguridad. Las responsabilidades de seguridad de TI están asignadas, pero no se hacen cumplir de manera consistente. Existe un plan de seguridad de TI, que impulsa el análisis del riesgo y soluciones de seguridad. El reporte de seguridad de TI está concentrado en TI, en lugar de concentrarse en el negocio. Se realizan pruebas Ad hoc de intrusión.

**4.- Administrado y medible** Las responsabilidades de la seguridad de TI están claramente asignadas, administradas y se hacen cumplir. El análisis de riesgo e impacto de seguridad se lleva a cabo de manera consistente. Las políticas y prácticas de seguridad son completadas con bases específicas de seguridad. Los reportes de conocimiento de seguridad se han vuelto obligatorios. La identificación, autenticación y autorización de usuario se está estandarizando. Se está estableciendo la certificación de seguridad del personal. La prueba de intrusión es un proceso estándar y formalizado que conduce a mejoras. El análisis costo / beneficio, que soporta la implementación de medidas de seguridad, es cada vez más utilizado. Los procesos de seguridad de TI son coordinados con la función general de seguridad de la organización. El reporte de seguridad de TI está vinculado con los objetivos del negocio.

**5.- Optimizado** La seguridad de TI es una responsabilidad conjunta del negocio y de la administración de TI y está integrada con objetivos de seguridad corporativa del negocio. Los requisitos de seguridad de TI están claramente definidos, optimizados e incluidos en un plan verificado de seguridad. Las funciones de seguridad están integradas con aplicaciones en la etapa de diseño y se les puede pedir a los usuarios finales que rindan cuenta de la seguridad a la administración. El reporte de seguridad de TI provee un aviso anticipado del riesgo cambiante y emergente, usando métodos activos automatizados de monitoreo para los sistemas críticos.

Los incidentes son prontamente resueltos con procedimientos formalizados de respuesta a incidentes soportados por herramientas automatizadas. Las evaluaciones periódicas de seguridad evalúan la efectividad de la implementación del plan de seguridad. Se recoge y analiza sistemáticamente la información sobre nuevas amenazas y vulnerabilidades, y se comunican e implementan prontamente los controles adecuados de mitigación. La prueba de intrusión, análisis de las causas originarias de los incidentes de seguridad y la identificación proactiva del riesgo es la base para el mejoramiento continuo. Los procesos y las tecnologías de seguridad están integrados en toda la organización.

El resultado de la medición de cada uno de los objetivos de bajo nivel nos llevará a la medición de la madurez del proceso DS5[26]. Esta calificación es mejorable en el tiempo según el estado deseado y garantizando que los objetivos de control se seguirán conforme a lo establecido.

Tanto ITIL, COBIT y 17799 son perfectamente compatibles e independientemente de cuál se implemente es muy seguro que se esté cumpliendo algún ítem u objetivo de control de las otras 2.

[26] Dentro del dominio Delevery and Suport (DS) se encuentra el subproceso DS5, Garantizar la Seguridad de los Sistemas.

## 1.4. PRINCIPALES INCIDENTES DE SEGURIDAD

Año tras año la CSI/FBI[27] publica un estudio relacionado con los incidentes de seguridad que sufren las empresas u organizaciones principalmente situadas en los Estados Unidos de Norteamérica, es interesante observar los hallazgos realizados desde el año 2004 al 2008:

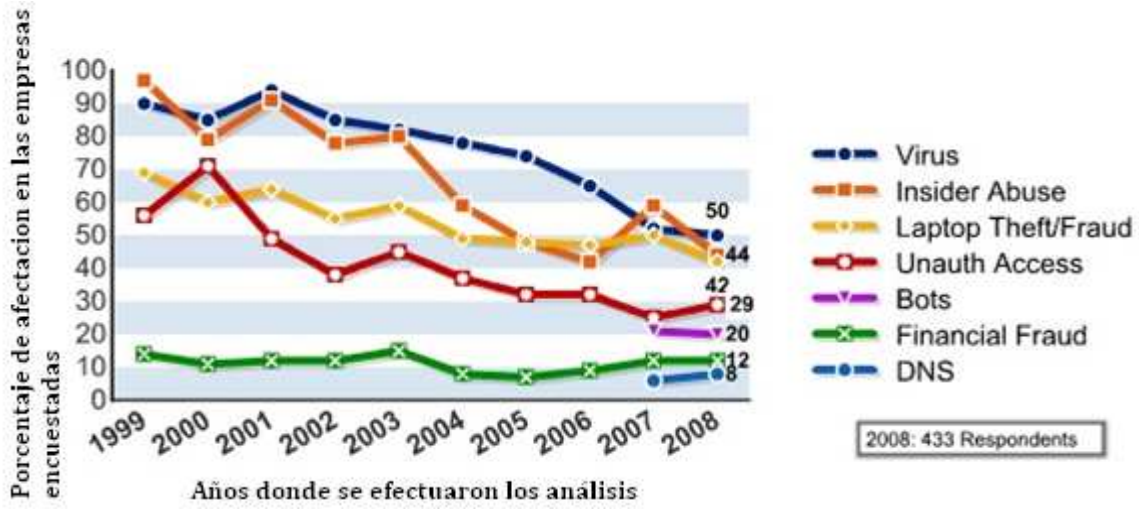



Fig 1.3, cuadro descriptivo de la evolucion de incidentes de seguridad reportados desde el año 1999. [28]

| | Incidente | 2004 | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|---|
| 1 | Denegación de servicios | 39% | 32% | 25% | 25% | 21% |
| 2 | Robo de portátiles | 49% | 48% | 47% | 50% | 42% |
| 3 | Fraude de telecomunicaciones | 10% | 10% | 8% | 5% | 5% |
| 4 | Acceso no autorizado | 37% | 32% | 32% | 25% | 29% |
| 5 | Virus | 78% | 74% | 65% | 52% | 50% |
| 6 | Fraude Financiero | 8% | 7% | 9% | 12% | 12% |
| 7 | Abuso Interno | 59% | 48% | 42% | 59% | 44% |
| 8 | Penetración a sistemas | 17% | 14% | 15% | 13% | 13% |
| 9 | Sabotaje | 5% | 2% | 3% | 4% | 2% |
| 10 | Robo/Perdida de información de | 10% | 9% | 9% | 8% | 9% |

[27] La Oficina Federal de Investigación (FBI) publica, en cooperación con el Computer Security Institute (CSI), el informe sobre actividades de investigación relacionadas con los incidentes de seguridad en empresas.

[28] Gráfica tomada del informe CSI/FBI Computer Crime and Security Survey del año 2008.

| | | | | | | |
|---|---|---|---|---|---|---|
| | propietario | | | | | |
| 11 | Abuso de redes inalámbricas | 15% | 16% | 14% | 17% | 14% |
| 12 | Cambios en pag. WEB | 7% | 5% | 6% | 10% | 6% |
| 13 | Mal uso de pag. WEB | 10% | 5% | 6% | 9% | 11% |
| 14 | Bots[29] | | | | 21% | 20% |
| 15 | Ataques a DNS's | | | | 6% | 8% |
| 16 | Abuso de mensajeria instantanea | | | | 25% | 21% |
| 17 | Robo de password | | | | 10% | 9% |
| 18 | Robo/Perdida de informacion de clientes | | | | 17% | 17% |
| 19 | Desde dispositivos moviles | | | | | 8% |
| 20 | Desde otras fuentes | | | | | 8% |

Tabla 1.4, Cuadro descriptivo de los incidentes de seguridad reportados en las empresas encuestadas en el informe CSI/FBI Computer Crime and Security Survey del año 2008, desde el año 2004.

De la FIG 1.3 y de la Tabla 1.4 se puede observar lo siguiente:

- Una disminución considerable de los incidentes de seguridad relacionados con virus, del 78% al 50%, y de los incidentes relacionados con el abuso interno, del 59% al 44%
- Aparición de nuevos incidentes de seguridad en los años 2007 y 2008:
  - Bots
  - Ataques a DNS
  - Abuso de mensajeria instantánea
  - Robo de passwords
  - Robo/pérdida de información de clientes.

Las apariciones de nuevas amenazas en cuanto a la seguridad de la información ha obligado que las empresas aumenten la tecnología asociada para evitar que los incidentes ya experimentados se vuelvan a repetir. De 11 tipos de tecnologías

29 referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC: Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será muchos más simple. Sus fines normalmente son poco éticos.

usadas en el año 2005, se observa un aumento considerable de uso tecnológico en un 109% para el año 2008 (ver tabla 5); aumentando también el nivel de complejidad de las herramientas de Firewalls hasta sistemas más sofisticados como el IPS (sistema de prevención de intrusos).

| Tecnologías Usadas | 2005 (%) | 2006 (%) | 2007(%) | 2008(%) |
|---|---|---|---|---|
| Firewall | 97 | 98 | 97 | 94 |
| Antivirus | 96 | 97 | 98 | 97 |
| VPN | | | 84 | 85 |
| Antispyware | | 79 | 80 | 80 |
| IDS | 72 | 69 | 69 | 69 |
| Prevención de fuga de información | | | | 38 |
| Herramientas especificas de virtualización | | | | 29 |
| Web/filtro de URL | | | | 61 |
| Listas de control de accesos | 70 | 70 | 56 | 50 |
| Encriptar la data en tránsito | 68 | 63 | 66 | 71 |
| Vulnerabilidades, administración parches | | | 63 | 65 |
| Cuentas estáticas de acceso/passwords | | | 51 | 46 |
| Software de administración de logs | | 41 | 44 | 51 |
| firewall de aplicación | | 39 | 45 | 53 |
| Herramientas forenses | | 38 | 40 | 41 |
| Sistemas de seguridad especializados en wireless | | 32 | 28 | 27 |
| Seguridad en puntos finales | | 31 | 27 | 34 |
| Cuentas reusables/loggin y passwords | 52 | 46 | - | - |
| Encriptar archivos | 46 | 48 | 47 | 53 |
| Smart cards, tokens etc.. | 42 | 38 | 35 | 36 |
| PKI | 35 | 36 | 32 | 36 |
| IPS | 35 | 43 | 47 | 54 |
| Biométricos | 15 | 20 | 18 | 23 |

Tabla 1.5. Cuadro descriptivo donde se detalla la evolución de las tecnologías usadas por las empresas encuestadas en el informe en el informe CSI/FBI Computer Crime and Security Survey del año 2008, desde el año 2004.

El uso de un firewall, que se ha mantenido constante en cuanto a su utilización a nivel empresarial, se ha vuelto ineficiente para evitar los incidentes actuales de seguridad en las empresas. Los firewalls deniegan o permiten el acceso dependiendo solamente de una IP-puerto-protocolo, pero la sagacidad de los intrusos internos o externos ha permitido enmascarar tráfico no válido dentro de trafico IP valido, para lo cual el firewall ya no representa una barrera eficaz para evitar los incidentes de seguridad; por ejemplo en los ataques conocidos como XXS Cross Site Scripting, SQL injection que entran directamente desde la capa de aplicación tres capas arriba donde suelen situarse las reglas de protección del firewall.

Lo mismo sucede con el antivirus y los ataques de día cero, donde la tecnología de virus se vuelve inocua e ineficiente, más aún cuando depende de actualizaciones y parchado de software independiente de la plataforma de antivirus; el último incidente Conficker. Para marzo de 2009 el 6% de los computadores en el mundo habían sido víctimas de este virus[30], su forma de contagio USB y a través de la red, explotando una vulnerabilidad en los sistemas operativos de Windows y la funcionalidad “autorun” implementada por Microsoft.

Lo ataques a la información han ido evolucionando conforme la tecnología para evitarlos. En un principio los virus fueron creados con la finalidad de causar algún tipo de denegación de servicios a todo nivel, desde una PC del hogar hasta los super-servidores de las empresas, poco a poco se fue evolucionando hasta un ámbito un poco más lucrativo: el robo y venta de información

El robo de información es hoy por hoy uno de los principales riesgos que sufren las empresas, no es de extrañarse encontrar eventos relacionados con el robo de laptops, abuso de privilegios, accesos no autorizados. De la misma manera la utilización de tecnología asociada a evitar este tipo de incidentes ha aumentado

[30] Tomado del Government Computer News, http://gcn.com/Articles/2009/01/15/Conficker-worm-still-lurks.aspx

se tiene por ejemplo firewall de aplicaciones, protección a las web/filtro, VPN, Prevención de fuga de información, vulnerabilidades/instalación de parches y un aumento considerable en la utilización de IPS´s. Este aumento tecnológico en las empresas demuestra la preocupación que estas tienen en el aspecto de seguridad debido fundamentalmente a las pérdidas asociadas que las empresas tienen cuando sufren algún incidente relacionado con la seguridad de información. La grafica muestra las pérdidas asociadas con incidentes de seguridad de la información:


Fig 1.4, cuadro descriptivo de la evolucion de pèrdidas
relacionadas con incidentes de seguridad reportados desde el año 1999.[31]

La cantidad de pérdidas experimentadas debido a incidentes de seguridad tuvo su más alto nivel en el año 2001 desde ahí y con las medidas implementadas y tecnología se han ido disminuyendo hasta el año 2006. Sin embargo ha existido un pequeño repunte en el 2007 y 2008 debido principalmente a la aparición de nuevas vulnerabilidades y métodos de ataque (ver tabla 5).

Todos los incidentes de seguridad, incluidos los señalados anteriormente se materializan debido a 2 factores conocidos como amenaza y vulnerabilidad.

[31] Grafica tomada del informe CSI/FBI Computer Crime and Security Survey del año 2008.

La probabilidad de que la amenaza se materialice en la empresa se la conoce como Riesgo. El Riesgo por lo tanto se lo disminuye cerrando las vulnerabilidades y lo que las organizaciones pretenden o buscan dentro del ambiente de seguridad es simplemente que ningún incidente relacionado con la confidencialidad integridad o disponibilidad de la información devenga en una paralización de las operaciones de la empresa o en algún tipo de pérdida que disminuya sus ganancias.

En un estudio realizado por la Trend mircro systems se encontró las siguientes, amenazas de seguridad en el año 2009:

1) **Web 2.0**: será el blanco de los creadores de código malicioso. Los logros y metas, así como los peligros de las aplicaciones Web 2.0 continuarán siendo un problema en 2009. Los hackers se valdrán de técnicas, como los IFRAMES, para camuflar el malware bajo la apariencia de código normal, y también seguirán utilizando los navegadores de Internet y otras aplicaciones habilitadas vía web, tales como Flash y los reproductores de medios, entre otros, como vectores de infección. El lanzamiento de Google Chrome, el próximo lanzamiento oficial de Internet Explorer y el crecimiento de las aplicaciones de navegador como plataforma, por ejemplo, Microsoft Silverlight y Adobe Integrated Runtime, servirán como nuevos puntos de explotación.

2) **Sistemas operativos alternativos:** todo lo bueno tiende a terminar, incluyendo la supuesta seguridad de las plataformas “alternativas”. Las amenazas que explotan las vulnerabilidades de los sistemas operativos alternativos experimentarán un crecimiento, especialmente con la creciente popularidad de Mac y Linux (este último por la explosión del mercado de los netbooks).

3) **Microsoft, el eterno objetivo:** los autores de código malicioso tienen una especial fijación con Microsoft. Seguramente veremos actividad maliciosa alrededor de la liberación de Windows 7 cuando, sin duda, los criminales probarán cualquier afirmación de que el nuevo Windows está “libre de virus”. El código malicioso de

prueba de concepto también explotará Microsoft Surface, Silverlight y Azure. Asimismo, los ciber criminales seguirán empleando un método más profesional para aprovechar la ventana de oportunidad de explotación presentada por el calendario mensual de “Patch Tuesday” (Martes de Parches) de Microsoft, en el que las explotaciones de día cero seguirán provocando problemas a los usuarios del gigante de Redmond.

4) **La ingeniería social alcanzará su cúspide**: los ciber criminales seguirán aprovechando eventos, celebridades y figuras políticas como cebo de la ingeniería social. El código malicioso relacionado con las elecciones en Estados Unidos seguirá causando problemas incluso después de que el presidente electo haya ocupado el Despacho Oval, mientas que los jugadores que esperan la llegada de “Starcraft 2” y “WoW: Wrath of the Lich King” deberán tener especial cuidado. Por otro lado, y aprovechando la crisis financiera global, los ciber-criminales sacarán partido del panorama económico creando correos electrónicos con el tema de la economía como gancho, falsificarán cupones electrónicos, así como esquemas de trabajo en casa y realizarán otros esfuerzos para aprovechar el deseo de los consumidores de ahorrar dinero.

5) **Guerras de bandas electrónicas:** los investigadores de seguridad son testigos de las guerras de virus, guerras de gusanos y guerras de botnets – debido a la creciente competencia por obtener ganancias financieras del phishing y el fraude-. Además, están viendo la consolidación de bandas de ciber-criminales, y las mejoras en soluciones de seguridad. Asimismo, en 2009 veremos una creciente competencia entre Europa Oriental y China para determinar qué criminales y de qué país serán los primeros en incluir las explotaciones más recientes en sus kits de explotación.

6) **La cruda realidad de las amenazas virtuales:** muchas amenazas del mundo real también existen en el mundo virtual. Ya que los criminales necesitan grandes audiencias para perpetrar sus

crímenes, han comenzado a hacer presa a los residentes de los mundos virtuales y a los jugadores de los juegos online. El número y tipo de amenazas en el entorno virtual incluye una serie de comportamientos humanos y pueden ser tan inocentes como compartir contraseñas entre socios; tan sofisticados como un fraude en bienes raíces real; y tan malicioso como las bandas delictivas buscando nuevas presas. Veremos que las amenazas virtuales se convertirán en uno de los mayores problemas en 2009.

7) **DNS roto:** los ciber-criminales aprovecharán los huecos identificados en el registro de DNS (sistema de nombres de dominio) para perpetrar sus delitos. Según los expertos, ya se están utilizando técnicas como el caché DNS envenenado para crear canales de comunicación encubiertos, medidas para eludir la seguridad y suministrar contenido malicioso. Si bien la comunidad de fabricantes de seguridad, incluyendo a Trend Micro, está trabajando estrechamente con los registros/registradores hasta donde les es posible, este es un problema que la ICANN (Corporación Internet para Nombres y Números Asignados) debe solucionar.

8) **La economía clandestina sigue floreciendo:** el ciber-crimen se ha convertido en un gran negocio y, desafortunadamente, 2009 será testigo de un crecimiento continuo. El aumento del código malicioso que roba información personal, bancaria y de tarjetas de crédito, continuará porque ahí es donde está el dinero y el crimen electrónico se mueve y se promueve simple y llanamente por razones económicas.

9) **Código malicioso más inteligente al alza:** los avances en tecnologías maliciosas son una apuesta segura ya que los autores de código malicioso siguen desarrollando y liberando código que busca evitar su detección y eliminación. Así, encontraremos más familias de código malicioso pero menos variantes, lo que hace más difícil que las compañías antivirus creen patrones heurísticos para

detectarlos. El mayor problema es el creciente tamaño y frecuencia de actualización de estos archivos de patrones que, de hecho, se ha convertido en un problema mayor que el mismo código malicioso.

10) **Compromiso y buenas intenciones:** no todas las noticias son malas. Los esfuerzos de la comunidad están surtiendo efecto y se está comenzando a reducir los vectores de amenazas. Los esfuerzos conjuntos están cada vez mejor planeados, coordinados y dirigidos, esto supone una bocanada de aire fresco en un movimiento que reclama actuar y no quedarse solo en el trabajo de escritorio.

De todos los estudios mostrados se observa un rápido cambio de amenazas a nivel mundial ya que el avance tecnológico que experimenta la humanidad así lo permite. Mientras que en un principio con un firewall y antivirus las empresas podían sentirse seguras la realidad en la actualidad no permite tener este sentido falso de seguridad. Que puede hacer un firewall frente a un ataque de ingeniería social? O que puede hacer un antivirus frente a un ataque de SQL injection? La tecnología se vuelve obsoleta frente a ataques informáticos modernos donde en algunas ocasiones las barreras tecnológicas no pueden hacer frente a una cultura organizacional deficiente.

¿Que pueden entonces hacer las empresas para estar a la par, seguir este avance tecnológico de las amenazas y ver si su empresa u organización son susceptibles a ellas? Mediante la medición de los procesos de seguridad que muestre su exposición al riesgo de seguridad, COBIT.

# CAPITULO 2: AUDITORIA AL PROCESO DS5 DE COBIT

## 2.1. INTRODUCCIÓN

Luego de la fusión de las dos compañías, descrita en el capitulo anterior, Andinatel S.A. pasó a formar parte de la Corporación Nacional de Telecomunicaciones, que de aquí en adelante se le denominará CNT S.A., con la participación de Pacifictel S.A.. Andinatel S.A. en este contexto no sufrió cambios que desestabilizarán sus estructuras internas, en cambio que sus procesos y procedimientos fueron generalizados para toda la organización. Esto no fue la excepción dentro del entorno de TI ya que la mayoría de aplicaciones necesariamente tenían que replicarse en la zona de la ex Pacifictel S.A. si es que se quería alcanzar el objetivo antes mencionado.

Por todo lo expuesto y debido a que la auditoria fue elaborada en un periodo anterior a la conformación de la Corporación Nacional de Telecomunicaciones y ya que los cambios internos no desestabilizaron las estructuras internas de Andinatel S.A., cuando se haga referencia a la Gerencia Nacional de TI tendrá que entenderse que en ese entonces se denominaba Vicepresidencia de Sistemas.

### 2.1.1. DETERMINACIÓN DEL ALCANCE

La Gerencia Nacional de TI brinda servicios que dan soporte a una serie de procesos internos dentro de la organización. Para el correcto funcionamiento de cada uno de estos servicios se administra infraestructura que soporta la alta transaccionalidad derivada de las actividades propias de la compañía, como aplicaciones, servidores, redes y bases de datos.

La red que permite la interconectividad con todos los elementos que son parte de la provisión de servicios internos[32] está centralizada en cuanto su administración y manejo en la Gerencia Nacional de TI, que de aquí en adelante se denominará la

[32] Provisión de servicios como la recaudación, facturación, acceso a balances financiero, para citar algunos.

red de GNTI; sin embargo se tiene otras redes dentro de la misma institución que son administradas por otras unidades de negocio, como por ejemplo la red de la ex andinanet y la red de ex andinadatos, que son administradas por la Gerencia Nacional de Operaciones.

La red de GNTI está estructurada como lo muestra la FIG 2.1 y consta de redes externas para conexiones con bancos y entidades como el Servicio de Rentas Interna -SRI-, Superintendencia de Telecomunicaciones -SUPTEL- y la compañía de telefonía celular Alegro PCS. Posee una zona desmilitarizada -DMZ- [33]donde se sitúan los servidores WEB para acceso desde el internet. Todas las conexiones antes descritas están protegidas, para el acceso interno mediante un firewall y un sistema de prevención de intrusos.

Dentro de la estructura de la red interna se tienen interconectadas las sucursales de las diferentes provincias del país, así como las sucursales de la provincia de Pichincha. La red de GNTI está segmentada en redes LAN virtuales[34] de voz, video y datos. En la red interna mostrada en la FIG 2.1, se encuentran además las distintas aplicaciones y sus elementos relacionados como bases de datos y servidores.

[33] Es una red local que se ubica entre la red interna de una organización y una red externa, es la zona donde las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones **desde** la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

[34] Son redes lógicamente independientes dentro de una misma red física

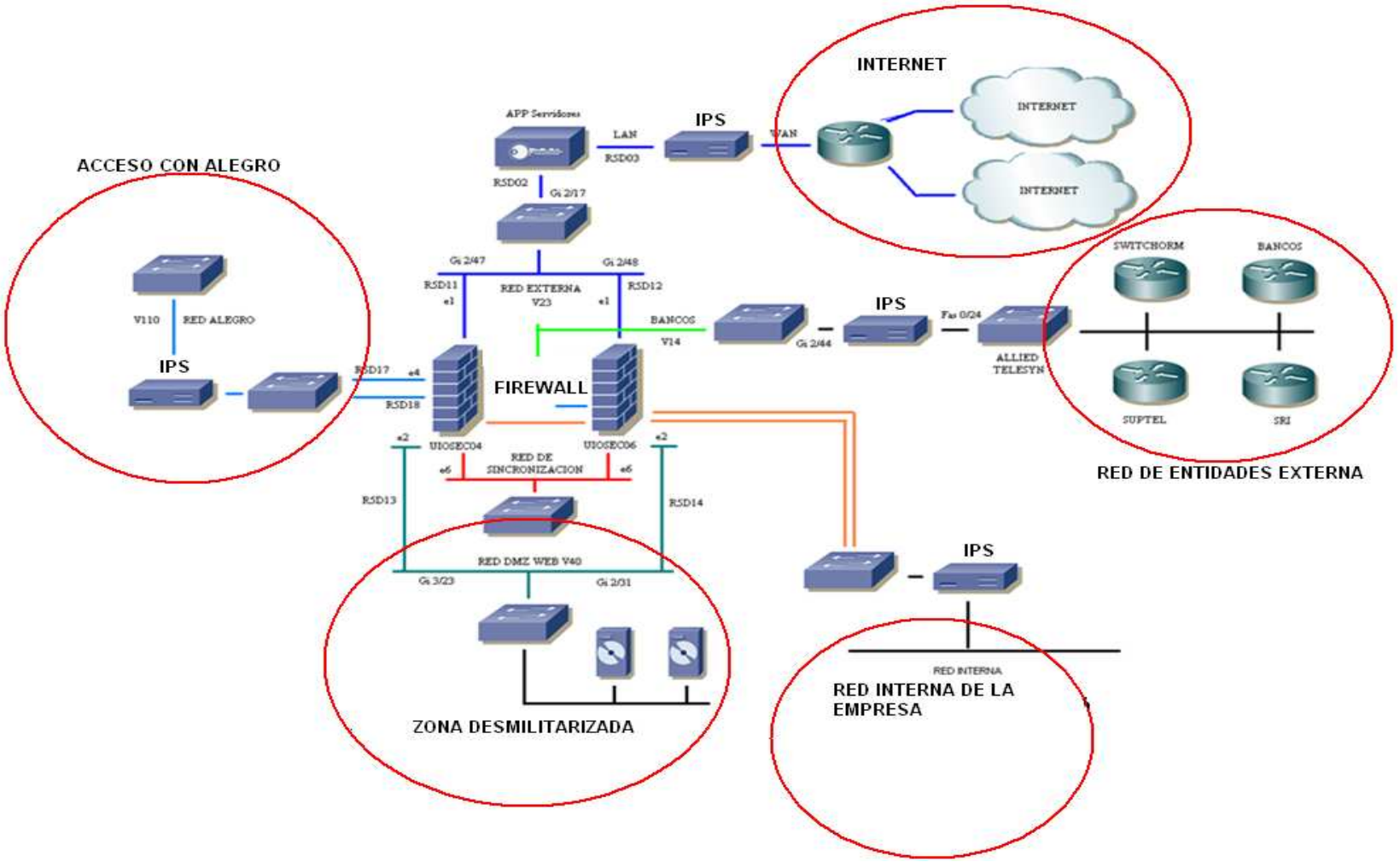



FIG 2.1 Diagrama de la red de GNTI

Los elementos que al momento la Gerencia Nacional de TI administra y que se encuentran al interior de la red GNTI son:

| BASES DE DATOS | |
|---|---|
| Versión de las bases de datos | Cantidad |
| Oracle 8i Enterprise Edition Release 8.1.7.4.0 | 4 |
| Oracle 8i Enterprise Edition Release 8.1.7.4.1 | 2 |
| Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 | 3 |
| Oracle Database 10g Enterprise Edition Release 10.1.0.4.2 | 3 |
| Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 | 11 |
| Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 | 3 |
| Oracle Database 10g Enterprise Edition Release 10.1.0.4.0 | 2 |
| Sybase IQ 12.7 | 2 |
| Oracle 8i Enterprise Edition Release 8.1.7.4.1 | 1 |

Tabla 2.1, enumeración de las bases de datos
administradas por la Gerencia Nacional de TI

| SERVIDORES | |
|---|---|
| Sistema operativo, servidores virtuales | Cantidad |
| Windows 2003 server | 13 |
| RedHat 4 | 7 |
| RedHat 3 | 4 |
| RedHat AS release 3 | 3 |
| RedHat 5,1 | 1 |
| Sistema Operativo, servidores físicos | Cantidad |
| Windows 2003 Server Enterprise edition | 8 |
| Windows 2003 Server | 31 |
| Windows 2000 Server | 14 |
| HP-UX | 2 |
| RedHat Enterprise Linux 4 | 9 |
| SUN Solaris 10 | 4 |
| HP-San Eva | 1 |
| Solaris | 8 |
| IBM-ESERVER | 7 |

Tabla 2.2, enumeración de los servidores
administrados por la Gerencia Nacional de TI

| EQUIPOS DE INTERCONECTIVIDAD | |
|---|---|
| Switches capa 3 | Cantidad |
| CISCO IOS v 12,2 | 6 |
| CISCO IOS v 12,1 | 1 |
| Routers | Cantidad |
| CISCO IOS versión 12,4 | 11 |
| CISCO IOS versión 12,3 | 14 |
| CISCO IOS versión 12,2 | 19 |
| CISCO IOS versión 12,1 | 8 |
| CISCO IOS versión 12,0 | 14 |
| CISCO IOS versión 11,2 | 1 |
| Access Point | Cantidad |
| CISCO IOS versión 12,3 | 12 |

Tabla 2.3, enumeración de los elementos de interconectividad administrados por la Gerencia Nacional de TI

Debido a la alta cantidad de equipos disponibles y a la posterior auditoria que más adelante se realizará, es necesario aplicar un enfoque adecuado que garantice un buen resultado, de manera que se obtengan los resultados deseados. Recordemos que el objetivo de la seguridad de la información es garantizar la seguridad de los sistemas, pero no de todos; sino de la criticidad del activo. Los costos de seguridad que se implementen tienen que estar acorde a la criticidad de un servicio (de los elementos de configuración de un servicio)[35], o dicho de otra manera la seguridad o los niveles de seguridad acordes a los valores que los servicios y cada uno de sus elementos tienen para una organización. Pero: ¿Que es lo verdaderamente crítico? y ¿En donde debemos enfocarnos?.

En octubre del año 2007 se realizó un análisis que buscaba determinar los servicios críticos que presta la Gerencia Nacional de TI. Una vez terminado el proyecto se determinaron los siguientes servicios como críticos para la compañía:

[35] Elementos de configuración de un servicio dentro de ITIL, se denominan CI, Configuration ITEM`s por sus siglas en ingles, y son todos los elementos que hacen posible la prestación de un servicio, servidores bases de datos, redes inclusive el aplicativo base.

- Open Flexis: sistema que permite realizar la facturación de servicios de la compañía. Maneja temas relacionados con la provisión de servicios de telefonía fija, ordenes de trabajo, líneas disponibles, tráfico entre otros.
- SAFA: sistema dedicado para la facturación de servicios de internet y datos. Usado principalmente en las unidades de negocio antes denominadas andinanet y andinadatos.
- CallCenter, ContactCenter e IVR´s: es el sistema utilizado para la respuesta automática de llamadas telefónicas. Se encarga además de manejar las opciones telefónicas. Este sistema también es utilizado para manejar servicios de atención al cliente externo[36].
- AXIS.- sistema usado para la realización de ventas, pagos, cobros para los servicios de Internet
- Correo Electrónico: sistema utilizado para la provisión del servicio de mensajería electrónica a través de la red de la GNTI.
- Bonus: sistema usado para la facturación de cabinas telefónicas
- Datawarehouse, Sistema que brinda información en línea desde la facturación comercial hasta la provision de servicios que la compañía ofrece.
- SIGAC, sistema financiero de la compañía, usado para la contabilidad compras y manejo de activos.

Estos servicios tienen bases de datos y servidores, los cuales se muestran a continuación:

| APLICACIÓN | BASE DE DATOS | SERVIDOR |
|---|---|---|
| OPEN | ANDINA | F2N17, F3N33, F4N49 |
| SAFA | ANDINA | F2N17, F3N33, F4N49 |
| SERVICIOS CALL CENTER, CONTACT CENTER E IVR`S | ANDINA_104 | UIOSQL01 |
| AXIS | DBAXISP | BDDV880 |

[36] Hace referencia a la atención de los clientes de la compañía. Abonados que buscan ayuda cuando por ejemplo el servicio contratado de internet o línea telefónica esta interrumpido.

| | | |
|---|---|---|
| CORREO ELECTRONICO | BUZONES DE CORREO | UIOMAI02 |
| SARI | APLIPROD | UIOORA02 |
| DATAWAREHOUSE | SYBASE IQ | UIODWH01 |
| SIGAC | BDSIGACP | UIOBDD01 |

Tabla 2.4, Mapeo de aplicaciones, base de datos relacionadas, servidor

Para donde corresponda en el trabajo de auditoría que más adelante se realizará se utilizarán las aplicaciones y elementos de TI mostrados en la tabla 2.4, además de considerar la red de la GNTI. Por lo que el alcance de la auditoria quedaría estructurado de la siguiente manera:

| Requerimiento del proceso de auditoria | |
|---|---|
| Alcance de la auditoria | Servicios críticos de negocio dentro la Gerencia Nacional de TI |
| | Infraestructura donde se apoyan esos servicios |
| | Funciones, responsabilidades, estructura organizacional |
| Identificación de los requerimientos de información para el negocio | Relevancia para los servicios críticos de negocio |

Tabla 2.5, Alcance de la auditoria

### 2.1.3. DETERMINACIÓN DE CONTROLES A AUDITAR

Para realizar la auditoria, además del alcance (mostrado en la tabla 2.5), se necesita determinar los objetivos de control que deben cumplir los procesos, personas y tecnología para considerarlos seguros, al respecto CoBIT dentro del proceso DS5 “Garantizar la seguridad de los sistemas” expresa lo siguiente:

*“Salvaguardar la información contra uso no autorizado, divulgación, modificación, daño o pérdida* **a través de** *Controles de acceso lógico que asegure que el acceso a*

*sistemas, datos y programas está restringido a usuarios autorizados*, ***tomando en consideración****:*

- *· Autorización,*
- *· Autenticación,*
- *· Acceso,*
- *· Perfiles e identificación de usuarios,*
- *· Administración de llaves criptográficas,*
- *· Manejo, reporte y seguimiento de incidentes,*
- *· Prevención y detección de virus,*
- *· Firewalls.*[37] *“*

Como se explicó en el capítulo I, a esto CoBIT lo denomina objetivo de control de alto nivel. Los objetivos de control de bajo nivel por su parte (controles que van a ser evaluados en la auditoria, con la finalidad de corregir anomalía que impidan que el objetivo primario se cumpla) son los que a continuación se detallan y que constan dentro del proceso DS5:

***“ DS5.1 Administrar la seguridad de IT***

*Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.*

***DS5.2 Plan de seguridad IT***

*Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las*

[37] Tomado de CoBIT dentro del Proceso DS5 de CoBIT “Garantizar la Seguridad de los Sistemas”

*políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.*

***DS5.3 Administración de identidades***

*Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.*

***DS5.4 Administración de las cuentas de usuario***

*Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la compañía son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.*

***DS5.5 Pruebas, vigilancia y monitoreo de la seguridad***

*Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.*

***DS5.6 Definición de incidente de seguridad***

*Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.*

***DS5.7 Protección de la tecnología de seguridad***

*Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.*

***DS5.8 Administración de llaves criptográficas***

*Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento,*

*captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.*

***DS5.9 Prevención, detección y corrección de software malicioso***

*Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).*

***DS5.10 Seguridad de la red***

*Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.*

***DS5.11 Intercambio de datos sensitivos***

*Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen. "*

Tanto los objetivos de control de alto nivel como los de bajo nivel son evaluados sobre el alcance previamente establecido para poder realizar el trabajo de auditoría. Los objetivos de bajo nivel nos permiten ver el detalle de lo que dentro del Objetivo de control de alto nivel está sucediendo, en cambio que este último nos da la generalidad y nivel de madurez de todo el proceso en conjunto.

### 2.1.4. PRESENTACIÓN DE LA AUDITORIA

La auditoria va a tener dentro de su estructura de presentación lo siguiente:

**a.- Criticidad:** son los niveles de atención que se otorga a la problemática encontrada dentro del objetivo de control. Puede tener tres niveles que dependerán de la incidencia que tenga el problema dentro de la organización y están descritos a continuación:

- **Criticidad Baja. -** cuando el área de afectación contemple una o dos jefaturas de una Gerencia Nacional de la CNT S.A.
- **Criticidad Media. -** cuando el área de afectación contemple una Gerencia Nacional de la CNT S.A.
- **Criticidad Alta. -** cuando el área de afectación contemple a la CNT S.A.

Estos niveles también pueden entenderse como la prioridad que el negocio debe dar para la solución de la problemática encontrada. A una alta criticidad le debe corresponder una prioridad alta de atención.

**b.- Oportunidades de mejora:** problemas encontrados en cada uno de los sistemas, procedimientos y controles de la Gerencia Nacional de TI de acuerdo a CoBIT.
**c.- Criterio:** en este campo se exponen los criterios bajo los cuales se otorga el nivel de criticidad o el juicio de no conformidad con la problemática encontrada. En algunos casos estos criterios provendrán de CoBIT y en otros de las normas internacionales relacionadas con seguridad.
**d.- Causas:** en este campo se describen las causas que originan la problemática encontrada dentro de la organización.
**e.- Nivel de madurez del objetivo de control:** esta calificación estará dada por CoBIT que tal como se lo menciona en el capítulo 1(pag 24) estará divido en 5 niveles los cuales son:

*“* ***0.- Inexistente.*** *La organización no reconoce la necesidad de la seguridad de TI. Las responsabilidades y las obligaciones de reportar no están asignadas para asegurar la seguridad. No están implementadas medidas que soporten la administración de la seguridad de TI. No hay ningún reporte de seguridad de TI y ningún proceso de respuesta de las violaciones de seguridad de TI. Hay una carencia total de un proceso reconocible de administración de seguridad de sistemas.*

***1.- Inicial /Ad hoc*** *La organización reconoce la necesidad de la seguridad de TI, pero la conciencia de la seguridad depende de la persona. La seguridad de TI está resuelta de manera reactiva y no se mide. Las violaciones de seguridad de TI invocan respuestas de “señalamiento” si se detectan, porque las responsabilidades no están claras. Las respuestas a las violaciones de seguridad de TI son impredecibles.*

***2.- Repetible pero intuitivo*** *Las responsabilidades y obligaciones de la seguridad de TI están asignadas a un coordinador de seguridad de TI que no tiene autoridad de administración. La conciencia de seguridad es fragmentada y limitada. La información de seguridad de TI es generada, pero no es analizada. Las soluciones de seguridad tienden a responder de manera reactiva a los incidentes de seguridad de TI y adoptando propuestas de terceros, sin resolver las necesidades específicas de la organización. Se están desarrollando políticas de seguridad, pero aún se siguen usando habilidades y herramientas inadecuadas. El reporte de seguridad de TI es incompleto, engañoso y no es pertinente.*

***3.- Proceso definido*** *Existe conciencia de la seguridad y la misma es promovida por la administración. Se han estandarizado y formalizados reportes de conocimientos de la seguridad. Los procedimientos de seguridad de TI están definidos y encajan en una estructura para políticas y procedimientos de seguridad. Las responsabilidades de seguridad de TI están asignadas, pero no se hacen cumplir de manera consistente. Existe un plan de seguridad de TI, que impulsa el análisis del riesgo y soluciones*

*de seguridad. El reporte de seguridad de TI está concentrado en TI, en lugar de concentrarse en el negocio. Se realizan pruebas Ad hoc de intrusión.*

***4.- Administrado y medible*** *Las responsabilidades de la seguridad de TI están claramente asignadas, administradas y se hacen cumplir. El análisis de riesgo e impacto de seguridad se lleva a cabo de manera consistente. Las políticas y prácticas de seguridad son completadas con bases específicas de seguridad. Los reportes de conocimiento de seguridad se han vuelto obligatorios. La identificación, autenticación y autorización de usuario se está estandarizando. Se está estableciendo la certificación de seguridad del personal. La prueba de intrusión es un proceso estándar y formalizado que conduce a mejoras. El análisis costo / beneficio, que soporta la implementación de medidas de seguridad, es cada vez más utilizado. Los procesos de seguridad de TI son coordinados con la función general de seguridad de la organización. El reporte de seguridad de TI está vinculado con los objetivos del negocio.*

***5.- Optimizado*** *La seguridad de TI es una responsabilidad conjunta del negocio y de la administración de TI y está integrada con objetivos de seguridad corporativa del negocio. Los requisitos de seguridad de TI están claramente definidos, optimizados e incluidos en un plan verificado de seguridad. Las funciones de seguridad están integradas con aplicaciones en la etapa de diseño y se les puede pedir a los usuarios finales que rindan cuenta de la seguridad a la administración. El reporte de seguridad de TI provee un aviso anticipado del riesgo cambiante y emergente, usando métodos activos automatizados de monitoreo para los sistemas críticos.*

*Los incidentes son prontamente resueltos con procedimientos formalizados de respuesta a incidentes soportados por herramientas automatizadas. Las evaluaciones periódicas de seguridad evalúan la efectividad de la implementación del plan de seguridad. Se recoge y*

*analiza sistemáticamente la información sobre nuevas amenazas y vulnerabilidades, y se comunican e implementan prontamente los controles adecuados de mitigación. La prueba de intrusión, análisis de las causas originarias de los incidentes de seguridad y la identificación proactiva del riesgo es la base para el mejoramiento continuo. Los procesos y las tecnologías de seguridad están integrados en toda la organización. "*

El nivel madurez de un proceso está dado por las características que estén presentes en la organización, evaluando todo en conjunto tanto los objetivos de alto nivel como los de bajo nivel.

## 2.2. AUDITORIA AL PROCESO DS5 "GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS"

La Auditoria que se va a realizar tomará en cuenta los servicios críticos, el alcance, y los controles a auditar predefinidos en este mismo capítulo.

### 2.2.1. DS5.1 ADMINISTRAR LA SEGURIDAD DE IT

**CRITICIDAD:** ALTA

**OPORTUNIDADES DE MEJORA**:

- Dentro del organigrama institucional el Área de Seguridad Informática está por debajo de la Gerencia Nacional de TI, sin tener una independencia total del entorno de TI, lo que podría en ciertas circunstancias delimitar su accionar en virtud de conseguir que los objetivos de seguridad se cumplan.
- Falta de una alineación de los objetivos de negocio, con los objetivos de la Gerencia Nacional de TI y con los objetivos de seguridad que permitan guiar el accionar de las tareas y labores del área, y que se hallen condensadas en un plan de seguridad a mediano, corto y largo plazo.


FIG 2.2, Organigrama Institucional, tomado de la intranet de la compañía

- Ausencia de un análisis de riesgo tecnológico y organizacional que permita medir la exposición al riesgo que tiene la organización para cumplir sus objetivos y como estos riesgos son transferidos a tecnología. Esta falta de medición del riesgo no permite tener una protección adecuada a los activos críticos, enfocando los esfuerzos de seguridad en reducir estos riesgos.

***CRITERIO:***

La alineación de los objetivos de negocio con los objetivos de tecnología es esencial para poder determinar el rumbo que tecnología debe seguir para apoyar al negocio y cumplir con sus metas preestablecidas. La seguridad informática en este ámbito debe guiar este proceso implementando los controles adecuados evitando que se materialicen incidentes de seguridad que puedan impedir que los objetivos organizacionales se cumplan. El área de seguridad debe brindar la seguridad adecuada dependiendo del riesgo identificado y de su valor.

***CAUSA:***

Falta de una alineación estratégica entre negocio y tecnología, y la medición del riesgo tecnológico de esta alineación con la finalidad de cumplir los objetivos organizacionales.

### 2.2.2. DS5.2 PLAN DE SEGURIDAD IT

**CRITICIDAD:** ALTA

**OPORTUNIDADES DE MEJORA:**

- Actualmente no se posee una política y un plan de seguridad informática para toda la organización, por lo que cada una de las gerencias, pertenecientes a la Gerencia Nacional de TI, está tomando medidas de seguridad de manera separada, aislada y a propio juicio del personal a cargo de la administración de redes, administración de servidores, administración de bases de datos y de los administradores de aplicaciones.
- Los procedimientos levantados en la Gerencia Nacional de TI no reflejan una adecuada segregación de funciones y establecimiento de roles y responsabilidades más aún cuando se trata de procedimientos en los que se relacionan varias gerencias. Por lo que se evidencia la siguiente problemática:

    - ✓ Los controles que existen en los procedimientos no son los suficientes, y en los procedimientos donde existen su eficacia no es medida.
    - ✓ Falta de una revisión periódica del cumplimiento de los procedimientos.
    - ✓ No existe una adecuada asignación de responsabilidades sobre los dueños de los procedimientos

- La administración de seguridad no está abarcando la totalidad de los elementos que conforman la infraestructura tecnológica de la compañía,

cubriendo los elementos de configuración de un servicio; desde las aplicaciones hasta los elementos de conectividad.

- Los procedimientos y políticas son difundidos y comunicados a través de correos electrónicos que dirigen a los usuarios a repositorios alojados en la intranet organizacional. Es necesario tomar en cuenta que la compañía tiene alrededor de 2300 empleados de los cuales alrededor de 1300 poseen un computador, es decir que solamente el 56.52% de las personas tiene acceso a la difusión a través de ese medio.

***CRITERIO:***

La norma de seguridad ISO 17799:2005 indica lo siguiente en cuanto a la elaboración de una política de seguridad:

*"El documento debería contener como mínimo la siguiente información:*

*a) Una definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permita compartir la información (véase el capítulo de Introducción);*
*b) el establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información;*
*c) una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización, por ejemplo:*

*1) conformidad con los requisitos legislativos y contractuales;*
*2) requisitos de formación en seguridad;*
*3) prevención y detección de virus y otro software malicioso;*
*4) gestión de la continuidad del negocio;*
*5) consecuencias de las violaciones de la política de seguridad;*

*d) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad;*

*e) las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.*

*Esta política debería distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible."*

En el plan de seguridad se condensa la visión departamental y estratégica del área para enfrentar la problemática y la necesidad de cubrir los riegos identificados en un análisis previo, mediante la implementación de controles en un plan a corto, mediano y largo plazo.

***CAUSA:***
La falta de una política y un plan de seguridad IT, correctamente alineados a los requerimientos de negocio además de un análisis de riesgo institucional y un análisis de impacto.

### 2.2.3. DS5.3 ADMINISTRACIÓN DE IDENTIDADES

**CRITICIDAD:** ALTA
**OPORTUNIDADES DE MEJORA**:

1. Las aplicaciones críticas que administra la GNTI posee su propio esquema de roles, perfiles, y además de esquemas de autenticación de usuarios que van desde tablas de usuario-password almacenadas en una tabla de base de datos hasta la autenticación por medio de Active-Directory[38]. No existe

[38] término utilizado por Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP

documentación de la entrega de administración de la aplicación a un responsable. Todo lo antes descrito ocasiona la siguiente problemática:

- ✓ Falta de estandarización de nombres de usuario en las aplicaciones organizacionales.
- ✓ Falta de una aprobación formal para otorgar permisos de acceso basados en las responsabilidades de trabajo.
- ✓ El área de seguridad no implementa los accesos otorgados a las aplicaciones.

- No se encuentra documentación que evidencie que los accesos otorgados a las aplicaciones esté en función de las responsabilidades de trabajo a realizar dentro de la compañía.

***CRITERIO:***

La correcta clasificación de las actividades de trabajo con los permisos a otorgar para el acceso a una aplicación o sistema, aseguran que los usuarios manipulen o procesen sólo la información que necesitan. La identificación del responsable de la aplicación, así como involucrarse en los módulos e información que la aplicación posee brinda un filtro necesario para evitar que se otorguen permisos innecesarios.

***CAUSA:***

Falta de una normativa y política de acceso a las aplicaciones de la compañía, procedimientos estandarizados y centralización para la administración de identidades.

### 2.2.4. DS5.4 ADMINISTRACIÓN DE LAS CUENTAS DE USUARIO

**CRITICIDAD:** ALTA

**OPORTUNIDADES DE MEJORA**:

- El procedimiento para la creación modificación y eliminación de cuentas de usuario no tiene las suficientes autorizaciones y validaciones, permitiendo que de esta manera existan cuentas genéricas[39] y cuentas cuyas contraseñas nunca expiran.
- Se encontró que los usuarios comúnmente comparten claves de acceso. Existen cuentas de usuario que son usadas por más de una persona.
- No existe un estándar para nombrar usuarios en las aplicaciones. A pesar de la existencia de un estándar para nombres de usuarios dentro del Active Directory (primera letra del primer nombre, seguido del apellido completo, y en caso de repetición del nombre de usuario se tiene que poner la inicial del segundo nombre) este no es replicado a la mayoría de las aplicaciones o sistemas críticos.
- No existe un ente centralizador que administre los pedidos de acceso hacia las aplicaciones y/o sistemas. Este permiso lo da el administrador del aplicativo bajo la solicitud del gerente de un área requirente mediante la utilización de un formulario de acceso. El formulario llega a cada uno de los administradores quienes finalmente otorgan e implementan el acceso.
- Existen cuentas de usuarios pertenecientes a empleados que dejaron de laborar en la compañía y siguen teniendo permisos sobre las aplicaciones que antes eran parte de su uso diario, existen alrededor de 50 usuarios que ya no forman parte de la compañía y que sin embargo continúan teniendo acceso a las aplicaciones o sistemas.

[39] Cuentas que tienen un nombre general y que no pertenecen a ninguna persona en particular.

- Cada una de las aplicaciones maneja su propio esquema de autenticación con características de seguridad propias de cada uno, dentro de los cuales se tiene:
    - ✓ Active Directory, autenticación para red y algunos sistemas
    - ✓ Autenticación por tablas de base de datos, sistema Open, Sistema Sigac, sistemas AXIS
    - ✓ Autenticación Kerberos, sistema autenticación para el acceso wireless.

***CRITERIO:***

La generación de cuentas de usuario en una aplicación se establece en base a un estándar que pertenezca e identifique de manera única a un empleado de la compañía. Esto permite contar con la trazabilidad necesaria de las acciones realizadas por un usuario determinado. Los procedimientos de creación modificación y eliminación de cuentas deben cumplir al menos con lo que establece la norma técnica ISO/IEC 17799, traducción al español de norma ISO 17799:

*"Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se debería prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema."*

Toda creación de usuario debe tener al menos tres componentes que abalicen y aseguren la creación de cuentas en base a una política predefinida estos son:

- ✓ Solicitante, la persona que solicita el permiso y que cuenta con los avales necesarios para el acceso, como por ejemplo autorizaciones de los inmediatos superiores con firmas de aceptación,

- ✓ Autorizador, quien se encarga de autorizar el permiso a la aplicación que generalmente administra. La autorización está acorde a las funciones y responsabilidades de trabajo; y
- ✓ Creador, encargado de implementar los permisos en el sistema o aplicación.

Las actividades de estos tres actores debe contar con una correcta segregación de funciones que garantice que las responsabilidades de cada uno esté plenamente definidas.

***CAUSA:***

Falta de una política y procedimientos de seguridad que regularice las creaciones modificaciones y eliminaciones de las cuentas de usuario. El procedimiento que se genere de la implantación de esta regulación debe tener indicadores de eficiencia además de tomar en consideración un levantamiento de información, debidamente aprobada por la alta gerencia, donde se defina según los cargos-funciones del empleado en la compañía sus correspondientes permisos de acceso a las aplicaciones.

### 2.2.5. DS5.5 TESTEO DE SEGURIDAD, VIGILANCIA, Y MONITOREO

**CRITICIDAD:** ALTA

**OPORTUNIDADES DE MEJORA**:

- Los archivos de logs[40] generados en los servidores no son revisados periódicamente debido a la gran cantidad información que arrojan y a la complejidad inherente que poseen como por ejemplo los arrojados por las plataformas unix, hp-ux, Sun Solaris, sólo por mencionar algunos casos. La revisión de logs debe realizarse con un enfoque proactivo que permita

[40] Logs, término que hace referencia a archivos que son generados por eventos parametrizados en los diferentes sistemas. Estos eventos pueden ser por ejemplo fallas en los discos duros, intentos de acceso, errores al cargar servicios entre otros

determinar con suficiente anterioridad algún tipo de incidente relacionado con seguridad. Se realizaron pruebas sobre los elementos críticos descritos en la tabla 2.4, donde se incluyeron búsqueda de vulnerabilidades y accesos no autorizados, los administradores de los equipos en cuestión nunca se percataron de las pruebas ni tampoco dieron aviso del incidente.

- Se lanzó un escaneo de puerto previo a un ataque de denegación del servicio hacia dos direcciones de red, la primera dirigida hacia un servidor en la red interna y otro hacia la DMZ por medio de la utilización de la herramienta Nessus 3, con la finalidad de probar la funcionalidad de detección de los sistemas de seguridad. Como era de esperarse según el diagrama de red de la FIG 2.1 el IPS no puede detener ni detectar este tráfico como lo muestra la FIG 2.3.


FIG 2.3 Escaneo de vulnerabilidades sobre el servidor UIOBDD01(172.17.1.19), no detectado con el IPS. Bloqueo del escaneo a la dirección en la DMZ 192.168.20.15 por parte del IPS.

Este escaneo fue realizado a la UIOBDD01, un servidor de base de datos Oracle, como se puede ver en la pantalla el evento no fue registrado en el IPS (registro en tiempo real). El evento lanzado hacia los servidores WEB alojados en la DMZ fue el único que se registró.

- Se realizaron pruebas de seguridad para buscar vulnerabilidades en los sistemas críticos. El resultado arrojó una gran cantidad de vulnerabilidades relacionadas principalmente con la aplicación de parches de seguridad y existencia de servicios que al parecer no deben estar activos.

***CRITERIO:***

Las redes de comunicaciones, los servidores, bases de datos y aplicaciones tienen mecanismos de control que periódicamente están arrojando información acerca de eventos que se generan sobre distintos eventos de seguridad, los cuales deben ser revisados diariamente. Así mismo es necesaria una revisión de la arquitectura de de red desde el punto de vista de seguridad con la finalidad de que la mayor cantidad de eventos de seguridad sean controlados, monitoreados; donde las actividades de seguimiento y control puedan ser más efectivas.

***CAUSA:***

Falta de controles de seguridad en la red que permitan detectar eventos anómalos sobre los elementos de configuración de los servicios críticos de la compañía y falta de herramientas que permitan el análisis y consolidación de logs en servidores, bases de datos y red en tiempo real; todo esto soportado en una Política de Seguridad.

### 2.2.6. DS5.6 DEFINICIÓN DE INCIDENTES DE SEGURIDAD

**CRITICIDAD:** ALTA
**OPORTUNIDADES DE MEJORA**:

- No existe un procedimiento de manejo de incidentes de seguridad donde se determinen los criterios bajo los cuales se establecen o clasifican los incidentes de seguridad, permitiendo de esta manera determinar los niveles de criticidad en un evento determinado, así como los niveles de escalamiento para la solución y la generación respectiva de la documentación relacionada.

***CRITERIO*:**
El manejo y respuesta de incidentes permiten a una organización manejar y responder con efectividad cuando un evento negativo se materializa, continuar con sus operaciones en caso de una interrupción y/o violación a la seguridad de los sistemas.

***CAUSA:***
Falta de una política y guía para el manejo de incidentes.

### 2.2.7. DS5.7 PROTECCIÓN DE LA SEGURIDAD TECNOLÓGICA

**CRITICIDAD:** MEDIA
**OPORTUNIDADES DE MEJORA**:

- No existe evidencia de documentación de las configuraciones de seguridad en los equipos críticos de red como son los firewalls y el IPS que esté debidamente aprobada, lo mismo ocurre con el software antivirus y los filtros

antispam, esto permite que puedan realizarse cambios sobre los mismos sin que sean detectados.

***CRITERIO*:**
La documentación de las configuraciones de seguridad en una organización deben estar debidamente aprobadas por las autoridades, no pueden depender de una persona o área. Igualmente todos las modificaciones que se realicen sobre los parámetros de seguridad en los equipos deben reflejarse en actualizaciones de la documentación previo a un proceso de control de cambios.

***CAUSA:***
Falta de documentación sobre las configuraciones de seguridad implementadas en cada uno de los elementos de seguridad y sistemas de tecnologías de información.

### 2.2.8. DS5.8 ADMINISTRACIÓN DE LLAVES CRIPTOGRÁFICAS

La compañía no maneja llaves criptográficas. No se ha detectado su necesidad

### 2.2.9.DS5.9 PREVENCIÓN DE SOFTWARE MALICIOSO, DETECCIÓN Y CORRECCIÓN.

**CRITICIDAD:** ALTA
**OPORTUNIDADES DE MEJORA**:

- El antivirus de la compañía no está cumpliendo con su principal objetivo. Se han encontrado PC`s de usuario con virus que han sido detectadas por otras herramientas que no son parte de la suite adquirida por la compañía y que representan un potencial problema para la organización. Se pudo comprobar que esta falencia se debe a la no actualización de los agentes del antivirus debido a una mala configuración del sistema.

- Se hizo una revisión del software instalado en la compañía, en base a un listado proporcionado por la herramienta SMS de Microsoft[41]. En esta lista se pudo encontrar software en las PCs de usuario que no corresponde al utilizado o instalado por la compañía. Ninguno de estos programas tiene una aprobación formal para su instalación y utilización;

- No hay evidencia de la existencia de campañas de educación al usuario final sobre la protección de software malicioso, medios frecuentes de infección, riesgos relacionados, a los que constantemente el usuario final está expuesto en la organización.

- Se ha evidenciado la inexistencia de una política de implementación de parches de seguridad en la que en conjunto con el Gestor de cambios establezcan los controles y niveles de riesgo. La criticidad de la implementación de parches en alguno de los servidores y bases de datos de la compañía principalmente en los que soportan el Billing empresarial OSS/BSS no se lo ha hecho debido a la falta de soporte de la versión tanto de hardware y software que al momento de la revisión se disponían (UNIX 4.53 y Oracle 8i ambos descontinuados y sin soporte del proveedor).

***CRITERIO:***

La protección contra el software malicioso impide que programas como virus, spyware rootkits y accesos mal intencionados penetren a elementos críticos de la compañía. Los sistemas operativos, bases de datos se protegen de estos accesos mediante la instalación de parches de seguridad. Por otro lado los controles para detectar y corregir la presencia de software en la red de la compañía son necesarios para impedir que software no licenciado o potencialmente perjudicial para la compañía pueda ser instalado.

[41] Software utilizado para la toma de control de las PC´s de usuario en el área de Service-Desk

***CAUSA:***

Falta de controles efectivos en la detección y prevención de software malicioso así como el establecimiento de políticas y procedimientos para la implementación de parches de seguridad.

### 2.2.10. DS5.10 SEGURIDAD EN LA RED

**CRITICIDAD:** ALTA

**OPORTUNIDADES DE MEJORA**:

- En la FIG 2.1 se pueden visualizar las redes que se interconectan a la red de la compañía IPS[42], firewall, zona desmilitarizada red de bancos SUPTEL, Alegro etc. La protección de estas redes para la red de GNTI lo constituyen el firewall y el IPS cada uno situado de manera correcta, este último por delante del firewall. Sin embargo, el IPS donde está dispuesto no protege de ataques generados desde el interior de la misma red de GNTI. El IPS en el sitio en el que se encuentra evita que tráfico no autorizado ingrese a la red de la compañía y a la zona desmilitarizada donde reposan las aplicaciones web, en este arreglo de seguridad no se han contemplado los ataques o irrupciones internas, a pesar de que existe segmentación con VLANs.

- Para el acceso entre VLANS se posee configuradas listas de control de acceso restringiendo así el acceso no autorizado entre VLAN de voz, video y datos, sin embargo la conectividad hacia las VLAN de servidores es posible desde cualquier lugar dentro de la organización por temas relacionados con el rendimiento y productividad. Esto posibilita que personas internas a la institución puedan realizar acciones sobre los servidores de producción como

[42] IPS, Sistema de prevención de intrusos, impide el acceso no autorizado a sistemas compañíariales. Basa su accionar en la detección de firmas de ataques y/o en patrones de ataque.

escaneos de vulnerabilidades, correr exploits[43] sobre servidores o las aplicaciones, sistema operativo sin ser detectadas.

- Se ha determinado que la capacidad DHCP configurada, y los puntos de acceso a la red conectados a puertos libres de switches permiten que cualquier persona interna o externa al conectar un host en la red obtenga acceso a la misma y a la vlan de servidores aumentando así la probabilidad de accesos no autorizados. El riesgo es mayor si se conecta un Access Point, cualquier dispositivo que posea una tarjeta inalámbrica podría acceder a la red de la compañía debido a la capacidad DHCP.

***CRITERIO:***

El diseño de la red debe conjugar un buen balance entre los aspectos de funcionalidad y los de seguridad, logrando de esta manera entregar un servicio efectivo y de manera segura que evite accesos no autorizados e interrupciones en las actividades de la compañía.

***CAUSA:***

Diseño de la red con un enfoque en desempeño más que con un enfoque de seguridad. Falta de políticas de control de acceso a la red y herramientas que restrinjan el acceso a la red de la compañía a host no autorizados.

### 2.2.11. DS5.11 INTERCAMBIO DE INFORMACIÓN SENSIBLE

**CRITICIDAD:** MEDIA

**OPORTUNIDADES DE MEJORA**:

- La información contenida en el OSS/BSS compañíarial (OPEN) y relacionada con los intercambios de información para la consolidación de cuentas pagadas así como la información de recaudación se basa en software y criptografía

[43] Programas escritos con la finalidad de acceder a un sistema por medio de la explotación de alguna vulnerabilidad conocida.

propietaria de la compañía que provee este aplicativo, sin embargo no se ha llevado una clasificación de las transacciones sensibles para el negocio donde se contemple los casos donde se deba implementar controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

***CRITERIO:***

Las aplicaciones críticas de negocio que manejan la información de la compañía así como sus transacciones no deben ser susceptibles de manipulación y/o divulgación en el tránsito desde el cliente hacia el servidor, protegiendo así la confidencialidad e integridad de la información.

***CAUSA:***

Falta de clasificación de criticidad a nivel gerencial de las transacciones e intercambio de información sensible.

## 2.3. EVALUACIÓN DEL NIVEL DE MADUREZ DEL PROCESO DS5 "GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS"

La madurez del proceso se determina tomando como referente lo enunciado por COBIT. Por un lado conocemos que el nivel de seguridad no es "0 inexistente" ya que si existe un proceso de seguridad establecido. Tampoco el nivel de madurez se sitúa en "3 Proceso definido" ya que la falta de políticas ha impedido que los procedimientos se establezcan con esa base, y tampoco existe un plan de seguridad que impulse un análisis de riesgos y soluciones de seguridad. Por lo tanto, el nivel de madurez se debe situar en 1 ó 2.

El nivel de madurez no está situado en 1 ya que la responsabilidad de seguridad esta delegada a un administrador. Si bien es cierto existen características que son propias de un nivel inicial dentro de este proceso, una mayor coincidencia con las propiedades del nivel 2 se encuentran presentes. Aunque no se ha mencionado con

anterioridad algunas de las características del nivel 1 se encuentran implementadas como por ejemplo controles y métricas así como el establecimiento de responsabilidades en los procesos y procedimientos.

Las características del nivel 2 en cambio son más claras y evidentes como por ejemplo:

1. La conciencia de seguridad es fragmentada y limitada.
2. La información de seguridad de TI es generada, pero no es analizada.
3. Las soluciones de seguridad tienden a responder de manera reactiva a los incidentes de seguridad de TI y adoptando propuestas de terceros, sin resolver las necesidades específicas de la organización.
4. Se están desarrollando políticas de seguridad, pero aún se siguen usando habilidades y herramientas inadecuadas.

Por las razones antes expuestas el proceso de seguridad estaría situado en el nivel 2 de madurez.

# CAPITULO 3: MEJORAMIENTO DEL PROCESO DS5

## 3.1. PROPUESTA DE MEJORAMIENTO DEL PROCESO DS5

El mejoramiento del proceso de seguridad DS5 estará dado por un conjunto de políticas, procedimientos y soluciones de seguridad que estarán enmarcados dentro de lo establecido por CoBIT.

### 3.1.1. OBJETIVO

Mejoramiento del proceso DS5 de COBIT que actualmente se encuentra en el nivel 2 de madurez y pasarlo al nivel 3, por medio de un conjunto de soluciones procedimientos y políticas de seguridad.

### 3.1.2. ALCANCE

Todo el ámbito de la Gerencia Nacional de TI, sus gerencias y en cada una de las áreas de la compañía donde incida el proceso.

### 3.1.3. DESCRIPCIÓN DEL PROBLEMA ACTUAL

Una de las principales debilidades detectadas en la auditoria fue la falta de concienciación en materia de seguridad ya que no se ha llevado a cabo un plan para el adiestramiento del personal en esta materia. Los usuarios son la primera línea que el proceso de seguridad debe atacar, pues es aquí donde precisamente se generan y detectan los incidentes relacionados.

Uno de los principales problemas derivados de esta falencia se evidencia cuando los usuarios toman a su criterio y necesidad las medidas de protección para la información. Estas medidas pueden o no satisfacer las necesidades organizacionales y de seguridad de la información.

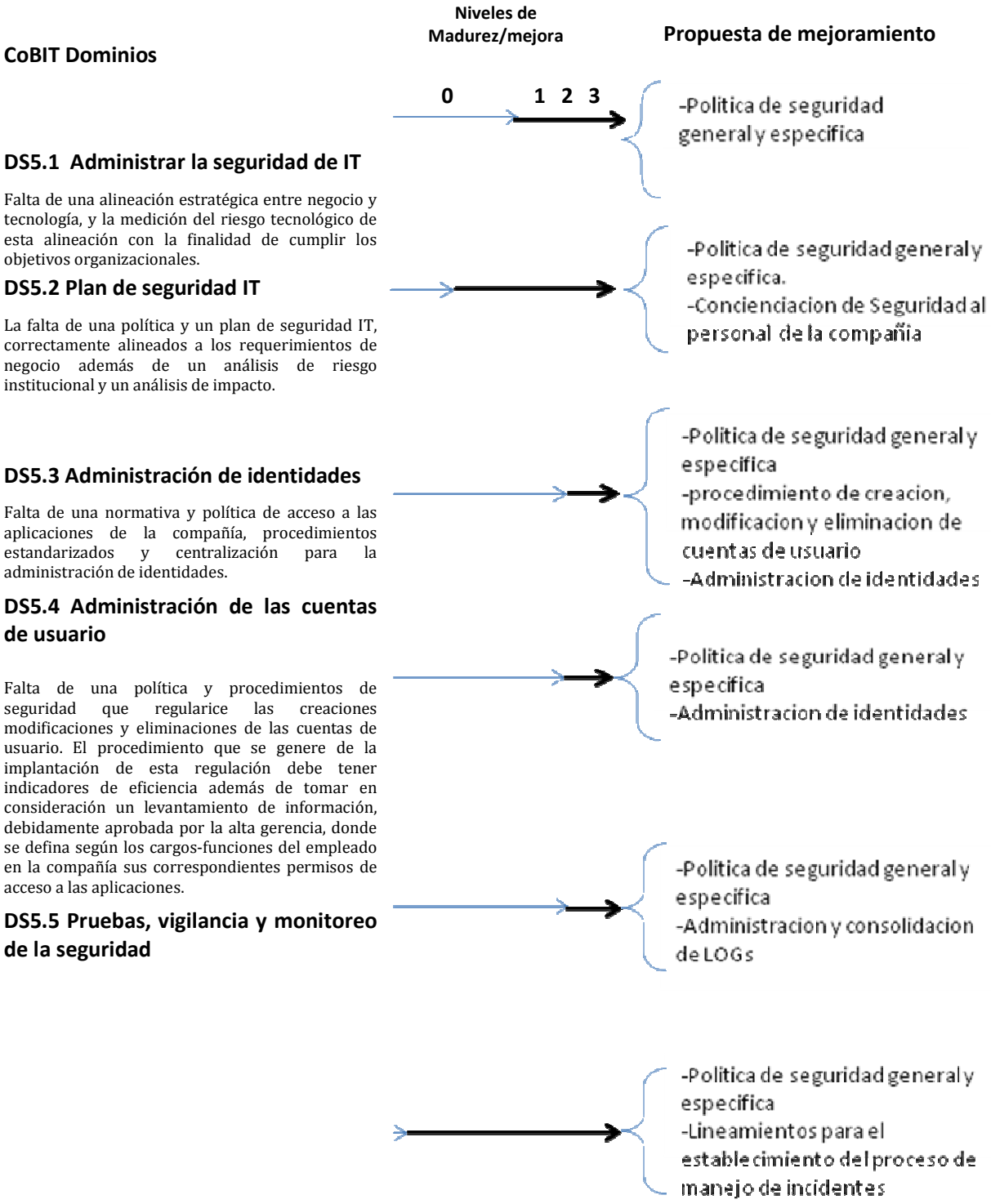
La problemática del control de acceso nace de una inadecuada segregación de funciones. Los permisos otorgados no van acorde a las responsabilidades que el personal necesita para el desarrollo de sus labores diarias.

En síntesis se pueden resumir los principales problemas encontrados en la auditoria de la siguiente manera:

- Inexistencia de una política de seguridad y políticas especificas
- Deficiente administración de los accesos lógicos a recursos.
- Controles inexistente para detección, manejo, reporte, solución y seguimiento de incidentes de seguridad.
- Debilidades en la detección de código malicioso.
- Debilidades en la seguridad de redes.
- Falta de clasificación de transacciones
- Falta de procedimiento para creación modificación de cuentas de usuarios
- Automatización de la creación de cuentas de usuario.

### 3.1.4. SOLUCIÓN PROPUESTA

En base a la problemática detectada en el capítulo II y expuesta a manera de resumen en la sección anterior se proponen las siguientes soluciones cuyo desarrollo se expondrá más adelante:


CoBIT Dominios
Niveles de Madurez/mejora
Propuesta de mejoramiento
0
1 2 3
DS5.1 Administrar la seguridad de IT
Falta de una alineación estratégica entre negocio y tecnología, y la medición del riesgo tecnológico de esta alineación con la finalidad de cumplir los objetivos organizacionales.
-Politica de seguridad general y especifica
DS5.2 Plan de seguridad IT
La falta de una política y un plan de seguridad IT, correctamente alineados a los requerimientos de negocio además de un análisis de riesgo institucional y un análisis de impacto.
-Politica de seguridad general y especifica.
-Concienciacion de Seguridad al personal de la compañía
DS5.3 Administración de identidades
Falta de una normativa y política de acceso a las aplicaciones de la compañía, procedimientos estandarizados y centralización para la administración de identidades.
-Politica de seguridad general y especifica
-procedimiento de creacion, modificacion y eliminacion de cuentas de usuario
-Administracion de identidades
DS5.4 Administración de las cuentas de usuario
Falta de una política y procedimientos de seguridad que regularice las creaciones modificaciones y eliminaciones de las cuentas de usuario. El procedimiento que se genere de la implantación de esta regulación debe tener indicadores de eficiencia además de tomar en consideración un levantamiento de información, debidamente aprobada por la alta gerencia, donde se defina según los cargos-funciones del empleado en la compañía sus correspondientes permisos de acceso a las aplicaciones.
-Politica de seguridad general y especifica
-Administracion de identidades
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
-Politica de seguridad general y especifica
-Administracion y consolidacion de LOGs
-Politica de seguridad general y especifica
-Lineamientos para el establecimiento del proceso de manejo de incidentes

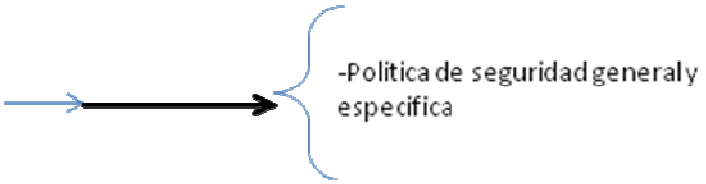
Falta de controles de seguridad en la red que permitan detectar eventos anómalos sobre los elementos de configuración de los servicios críticos de la compañía y falta de herramientas que permitan el análisis y consolidación de logs en servidores, bases de datos y red en tiempo real; todo esto soportado en una Política de Seguridad.

**DS5.6 Definición de incidente de seguridad**

Falta de una política y guía para el manejo de incidentes.

**DS5.7 Protección de la tecnología de seguridad**

Falta de documentación sobre las configuraciones de seguridad implementadas en cada uno de los elementos de seguridad y sistemas de tecnologías de información.




**DS5.8 Administración de llaves criptográficas**

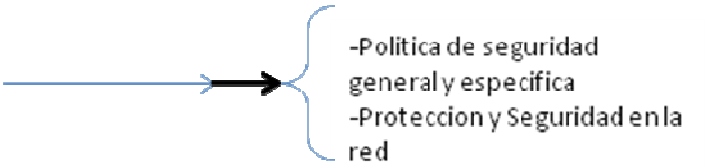
NO SE MANEJA LLAVES CRIPTOGRAFICAS

no se manejan llaves

**DS5.9 Prevención, detección y corrección de software malicioso**

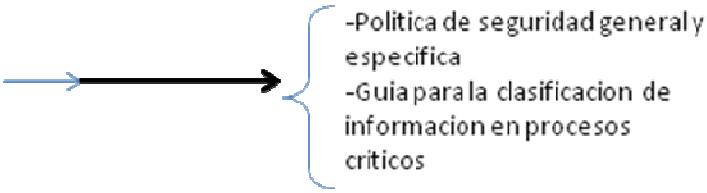

Falta de controles efectivos en la detección y prevención de software malicioso así como el establecimiento de políticas para la implementación de parches de seguridad.

**DS5.10 Seguridad de la red**




Diseño de la red con un enfoque en desempeño más que con un enfoque de seguridad. Falta de políticas de control de acceso a la red y herramientas que restrinjan el acceso a la red de la compañía a host no autorizados.

**DS5.11 Intercambio de datos sensitivos**




Falta de clasificación de criticidad a nivel gerencial de las transacciones e intercambio de información sensible.

## A.- POLÍTICAS DE SEGURIDAD.

Las políticas de seguridad brindan un marco de control para el establecimiento de medidas que buscan disminuir los riesgos internos de la compañía. Este marco brinda la base regulatoria por medio del cual se guiará el accionar de los usuarios en materia de seguridad. Los trabajadores por su parte se comprometen a cumplir lo

que en ella se estipula luego de que se aprobada por las máximas autoridades de la compañía.

Esta sección está dividida de la siguiente manera:

**A.1. Política General,** donde se expone un concepto general, alcance, el objetivo y el marco legal y regulatorio además de una generalidad de la política que engloba las políticas especificas que más adelante se desarrollan.

**A.2. Políticas Especificas,** que son las normativas aplicadas a un tema especifico que cubren la problemática encontrada en los capítulos anteriores esta sección se encuentra dividida además en:

**A.2.1. Administración de la seguridad.-** Se describe cómo se organiza la seguridad en la compañía para que tenga el empoderamiento necesario para cumplir y hacer cumplir lo estipulado en las políticas desarrolladas.

**A.2.2. Clasificación de la información.-** aquí se establece la necesidad de clasificar los activos de información y mantener este proceso continuo.

**A.2.3. Seguridad en el control de acceso.-** En esta sección se establecen los controles que deben tener las aplicaciones para dar acceso a los trabajadores así como el cuidado y características de password que deben ser implementadas. Este capítulo se subdivide en:

**A.2.3.1.** Manejo y utilización de passwords

**A.2.3.2.** El cuidado de passwords.

**A.2.3.3.** Control de acceso con terceros

**A.2.3.4.** Controles de acceso lógico

**A.2.4. Seguridad física y ambiental.-** Esta sección expone los controles físicos que debe poseer el centro de cómputo para permitir su acceso. Esta subdividida en:

**A.2.4.1.** Perímetro de seguridad

**A.2.4.2.** Controles de acceso físico a zonas restringidas

**A.2.5. Seguridad en la red.-** son los controles que se deben establecer en las redes para disminuir los riesgos asociados al acceso no permitido a recursos que ahí yacen, hace mención a una sección particular para la red inalámbrica.

**A.2.5.1.** Seguridad en la red inalámbrica:

**A.2.6. Seguridad de bases de datos, servidores, redes, lineamientos para los administradores.-** Son los lineamientos que deben seguir los administradores de recursos de TI para disminuir vulnerabilidades en sus recursos y administración.

**A.2.7. Seguridad en el sitio de trabajo.-** Normas para proteger los documentos en papel y dispositivos de almacenamiento removibles, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo

**A.2.8. Seguridad de software.-** Esta sección trata de la instalación de software no autorizado, el cuidado que se debe seguir para no infectar la red de la compañía con virus.

**A.2.8.1.** Software no autorizado

**A.2.8.2.** Virus y gusanos

**A.2.9. Comunicación sobre incidentes y brechas de seguridad.-** En esta sección se establece la necesidad de establecer la gestión de incidentes así como donde comunicarlos.

**A.2.10. Glosario de términos**

**A.2.11. Referencias a la ley.-** en esta sección se encuentran las referencias a leyes ecuatorianas que hacen relación a los delitos informáticos y de información, entre los cuales se encuentran:

**A.2.11.1.** Correo electrónico, firmas y mensajes de datos

**A.2.11.2.** Ley de propiedad intelectual

**A.2.11.3.** Ley de transparencia y acceso a la información pública

**B.- PROCEDIMIENTOS DE SEGURIDAD.**

Los procedimientos de seguridad desarrollados imponen contramedidas necesarias para ciertas actividades relacionadas principalmente con la creación modificación y eliminación de usuarios. No hay que olvidar que la manera más fácil de vulnerar o apropiarse de información es por medio del acceso a sistemas con cuentas y contraseñas de usuarios válidos.

Las guías o lineamientos dan las directrices por medio de las cuales se podrán realizar acciones para remediar algunos aspectos de seguridad que deben ser tomados en cuenta, como por ejemplo la clasificación de información que atraviesan los canales de comunicación.

En esta sección se desarrolla lo siguiente:

- Procedimiento de creación modificación y eliminación de cuentas de usuario
- Lineamientos para el establecimiento del proceso de manejo de incidentes.
- Guía para la clasificación de información en procesos críticos.

**C.-SOLUCIONES DE SEGURIDAD**.

Las soluciones de seguridad por su parte imponen controles a nivel de infraestructura de TI para evitar incidentes al interior de la compañía además de automatizar cierto tipo de actividades, por ejemplo la automatización de la creación de cuentas de usuario.

En esta sección se incluye:

- ADMINISTRACIÓN Y CONSOLIDACIÓN DE LOGS.- Proyecto que busca automatizar y mejorar la gestión de TI y la seguridad relacionada
- ADMINISTRACIÓN DE IDENTIDADES.- Proyecto que busca automatizar la provisión de cuentas de usuario.
- PROTECCIÓN Y SEGURIDAD EN LA RED:
    - PROTECCIÓN DE SERVIDORES EN LA RED.- Proyecto que busca disminuir vulnerabilidades encontradas en la red interna de la compañía
    - CONTROL DE ACCESO EN LA RED.- Proyecto para el control de acceso en la red de la empresa en base a políticas predefinidas de seguridad.
- CONCIENCIACIÓN DE SEGURIDAD AL PERSONAL DE LA COMPAÑÍA.- Directrices generales para el emprendimiento de campañas de educación al usuario en temas de seguridad.

## 3.2. DESARROLLO DE LA PROPUESTA DE MEJORAMIENTO DEL PROCESO DS5

### 3.2.1. POLÍTICA GENERAL DE SEGURIDAD

#### 3.2.1.1. Alcance:

La política de seguridad presente debe ser conocida y cumplida en todo el ámbito de la CNT S.A., abarca a sus recursos y a la totalidad de los procesos, ya sean internos o externos, en todas las sucursales del país, así como también terceros con los que se establezca alguna relación directa o indirecta, debiendo por lo tanto atenerse a las sanciones impuestas en la misma.

#### 3.2.1.2. Objetivo:

El propósito de este documento es definir los principios por los cuales todos los empleados de la CNT S.A. aseguran la información propiedad de la compañía, con el fin de precautelar la continuidad del negocio y minimizar el daño y el impacto de los

incidentes de seguridad, asegurando de esta manera la Integridad, Disponibilidad, y Confidencialidad de la información.

#### 3.2.1.3. Marco Legal:

Esta política de seguridad toma en cuenta las leyes vigentes en la República del Ecuador, relacionadas con la información y con los delitos que se pueden cometer con relación al mal uso de la misma.

La siguiente es una recopilación de las leyes vigentes relacionadas con la información:

- Ley de comercio electrónico, firmas y mensajes de datos
- Ley de propiedad intelectual
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Reglamento Interno de Trabajo

Al final de este capítulo se encontrará los extractos, de las leyes mencionadas, que tienen relación con la seguridad de la información.

#### 3.2.1.4. Concepto de seguridad de la información:

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversaciones.

La seguridad de la información se caracteriza aquí como la preservación de:

**i)** Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información

**ii)** Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos;

**iii)** Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

El negocio tiene sus propios requerimientos con respecto a información[44]:

**Efectividad**, la información tiene que ser relevante y pertinente para el negocio, entregada a tiempo, que sea consistente y que se la pueda usar.

**Eficiencia**, es la provisión de la información de una manera óptima, es decir de una manera productiva y económica.

**Cumplimiento**, relacionada con el acatamiento de leyes, regulaciones, compromisos contractuales, políticas y procedimientos para los cuales los procesos del negocio están sujetos externamente e internamente.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles aseguran que los objetivos específicos de seguridad de la organización se cumplan.

#### 3.2.1.5. Política:

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Compañía. Sin ellos la CNT S.A. perdería competitividad y quedaría relegada del negocio de las soluciones integrales de telecomunicaciones y por tal razón la Presidencia Ejecutiva, el Directorio y todas las personas que laboran, directa o indirectamente, tienen el deber de preservarlos, utilizarlos y mejorarlos, tomando las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

[44] Tomado de COBIT 4.0.

La información perteneciente la CNT S.A. debe protegerse de acuerdo a su valor e importancia indiferentemente de cómo esta se halle (en papel o en forma electrónica), o como se procesa (PC´s, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica).

La seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y los RRHH.

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 Compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido (Reglamento Interno de Trabajo, que fue aprobado por el ministerio de Trabajo) y si el caso amerita, se aplicará la rigurosidad de las leyes existentes de Ecuador que son afines a los temas tratados en esta Política[45].

### 3.2.2. POLÍTICAS DE SEGURIDAD ESPECIFICAS

#### 3.2.2.1. Administración de la Seguridad

El Directorio, la Presidencia Ejecutiva, Gerencias, y todos los niveles jerárquicos que sean parte de la organización y sea cual fuese su naturaleza de trabajo tienen la obligación de conocer y dar a conocer dentro del área a su cargo, así como también de cumplir, con estas Políticas de Seguridad.

La Gerencia Nacional de TI es responsable de la custodia de los datos y de la infraestructura informática de la CNT S.A., es decir debe tener todo el hardware de

[45] **Anexo A** que tiene referencias a las leyes de la República del Ecuador que tienen que ver con información y delitos Informáticos, dichas leyes son las siguientes.

- **a.** Ley de Comercio Electrónico, firmas y mensajes de datos;
- **b.** Ley de propiedad intelectual;
- **c.** Ley de Transparencia y acceso a la información pública;

servidores de aplicaciones centralizado en sus instalaciones ya sea de manera física o lógica.

La Seguridad de la Información está delegada a la Gerencia Nacional de TI, a través del Área de Seguridad Informática y será la responsable de la Seguridad de la información en la CNT S.A., además de asistir al personal de la CNT S.A. en materia de seguridad y junto con los propietarios de la información, analizará el riesgo de los activos de información de la Compañía y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma. Será además responsable de diseñar e implementar un plan de seguridad de la información que este alineado con los objetivos de negocio y tome en cuenta los riesgos existentes en la compañía. Así mismo se encargará de la revisión, que se dará en un periodo no mayor a un año desde la fecha de aprobación de la misma, así como también de emitir cambios cuando así lo amerite.

El Área de Seguridad Informática es la responsable de proveer ayuda y guía en todo lo relacionado con materia de seguridad, pero en última instancia los propietarios de la información [46]son los responsables de la implementación de esta Política de Seguridad sobre los activos bajo los cuales estos tienen control.

La Gerencia Nacional de TI deberá conformar un Comité de Seguridad IT de La CNT S.A. que se encargará principalmente de:

- Difusión y mejoramiento de la Política de Seguridad
- Revisión y seguimiento de las incidencias en la seguridad de la información;
- Respaldo de las iniciativas principales para mejorar la seguridad de la información.

[46] Propietarios de información en la Compañía es la alta Gerencia que se encuentra desde el Directorio Presidencia Ejecutiva y Gerentes, ellos son dueños de la información que es procesada dentro de sus áreas de responsabilidad y funciones a cargo

Este comité debe estar formado por los Gerentes o delegados de las gerencias que conforman la compañía.

**3.2.2.2.Clasificación de la información**

Los propietarios de la información y la criticidad de la misma están definidos en base al documento ¨*Plan para definir la sensibilidad, confidencialidad, y propiedad de la información*¨[47], mediante el cual cada una de las Áreas de la compañía llevará a cabo un inventario de activos, el mismo que deberá actualizarse y revisarse mínimo una vez en un periodo no mayor a un año y modificarse cuando este lo amerite, tomando en cuenta las leyes vigentes en el país y las necesidades inherentes en cada una de las áreas de la compañía.

Para lo referente a las normas institucionales que rigen sobre la información de la Compañía por favor referirse a la *Política de Acceso y Clasificación de la Información de La CNT S.A.*[48] en donde se describe básicamente la clasificación de la información tomando en cuenta las leyes vigentes sobre el acceso a la información pública.

Los usuarios, por su parte, que tengan acceso a información que ya ha sido clasificada como sensible y que por ende es de propiedad de la CNT S.A. o que la compañía le haya encargado, es su menester conocer y comprender los requerimientos de seguridad y tomar medidas para asegurarla sin importar el medio en el que esta se localice, ya sea:

- En medios impresos.

[47] Plan elaborado por la contraloría interna y aprobado por la Presidencia de Juan Esteban Arrellano, brinda una síntesis y lineamientos sobre los cuales clasificar la información de la compañía. Esta se basa en una política denominada "Política de acceso y clasificación de la información" para cumplir con la ley de transparencia y acceso a información pública.

[48] Plan elaborado por la contraloría interna y aprobado por la Presidencia de Juan Esteban Arrellano, brinda una síntesis y lineamientos sobre los cuales clasificar la información de la compañía. Esta se basa en una política denominada "Política de acceso y clasificación de la información" para cumplir con la ley de transparencia y acceso a información pública.

- En las computadoras.
- En la red (p.ej. voz, datos).
- En un medio magnético u óptico.(p.ej. discos duros, CD ROM, disquetes, memorias flash)
- En ambientes físicos de almacenamiento (p.ej. bodegas, archiveros)
- En la memoria de las personas.

Si algún usuario no es consciente de los requerimientos de seguridad para la información a la cual esta accediendo deberá poner en consideración su requerimiento lo antes posible al Área de Seguridad Informática, al igual que si una brecha de seguridad es encontrada o alguna violación que comprometa a la información crítica de la compañía.

Cada uno de los empleados nuevos o antiguos, necesitan firmar un contrato de confidencialidad de la información.

### 3.2.2.3.Seguridad en el control de acceso

Los usuarios sólo deben acceder a los sistemas para los cuales fueron autorizados por la autoridad competente de la CNT S.A. y de ninguna manera violentar las seguridades impuestas en los sistemas, ya sea por medio de alguna herramienta de software, o hardware o por medio de **ingeniería social**. [49]

Los accesos no autorizados, a sistemas a los cuales no fueron en un inicio acreditados, pueden ser sancionados de acuerdo a las leyes establecidas en el código penal [50] y/o con las sanciones correspondientes para el personal de la CNT S.A.

[49] Método por medio del cual se extrae información directamente de la persona de interés a través de algún tipo de engaño.
[50] Al final del capítulo un extracto de las leyes del Ecuador con relación a los delitos informáticos.

Para la creación, modificación, o eliminación de usuarios favor remitirse al ¨**Procedimiento de creación modificación y eliminación de usuarios** ¨.[51]

#### *3.2.2.3.1. Manejo y utilización de passwords*

Todos los usuarios a los que se les haya confiado una clave de acceso deben seguir los siguientes lineamientos:

a. La clave deberá ser mínimo de 8 caracteres siendo este entre letras y caracteres especiales, con un tiempo de caducidad de 3 meses.
b. Las cuentas de administración en los servidores en todas las Plataformas operativas (Windows, Unix, Linux HP-UX…) así como de las bases de datos y elementos de conectividad de la compañía deben tener una caducidad de 2 meses.
c. Las cuentas de usuario regulares de acceso a aplicaciones se bloquean automáticamente luego del cuarto intento fallido de acceso.

***El cuidado de las contraseñas.***

Los usuarios deben mantener las siguientes directivas:

d. Mantener las contraseñas en secreto.
e. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de sus contraseñas.
f. Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el literal a y además que:

- Sean fáciles de recordar.

[51] Procedimiento que se encuentra en la política de seguridad detallada en este capítulo.

- 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, fechas especiales, entre otras.

g. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
h. Cambiar las contraseñas del primer inicio de sesión o contraseñas que vienen por defecto incluidas en los sistemas críticos.
i. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro[52].
j. No guardar las contraseñas en una libreta de fácil acceso por personas ajenas, ni tampoco en un archivo digital, a menos que esté debidamente encriptado por algún método válido.
k. Notificar sobre cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad al Área de Seguridad informática y/o al área de Service-Desk, para proceder al cierre de la misma.

Para evitar el mal uso de sus cuentas y posibles sanciones, los usuarios deben cumplir con:

l. Concluir las sesiones activas al finalizar las tareas, y protegerse mediante un mecanismo de bloqueo de pantalla protegido por contraseña (ctrl.+alt+del y luego presionar la tecla ENTER).
m. 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, o protector de pantalla luego de

[52] En ocasiones los usuarios configuran funciones, aplicaciones, o conjunto de letras en una solo tecla o función. Estas teclas son F1, F2, etc., situadas en la parte superior de su teclado.

determinado tiempo de inactividad. Al momento de dejar el escritorio es obligatorio que se cierre la sesión para evitar el robo de la información o cualquier mal uso de su cuenta.

**Nota importante**: *Cualquier usuario al cual se le haya confiado un USER ID y PASSWORD para acceso a cualquiera de los sistemas que maneja la CNT S.A. y a los usuarios a los cuales se les haya confiado una tarjeta magnética serán los responsables por todas las actividades que se realicen con estos medios Por lo tanto los usuarios deben ser cautelosos en cuanto al robo o préstamo de estas tarjetas y/o passwords para evitar su uso no autorizado que puede acarrear algún tipo de sanción.*

#### *3.2.2.3.2. Control de acceso con terceros*

Cuando exista la necesidad de otorgar acceso a información de la CNT S.A., a terceros, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, y los responsables del acceso[53], llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

a. El tipo de acceso requerido (físico/lógico y a qué recurso).
b. Los motivos para los cuales se solicita el acceso.
c. El valor de la información.
d. Los controles empleados por la tercera parte.
e. La incidencia de este acceso en la seguridad de la información de la Compañía.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Compañía, se

[53] Según consta en el procedimiento de ¨ CREACIÓN, MODIFICACIÓN Y ELIMINICACIÓN DE CUENTAS DE USUARIO ¨

establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

- Personal de mantenimiento y soporte de hardware y software.
- Limpieza, guardia de seguridad y otros servicios de soporte tercerizados.
- Pasantías y otras designaciones de corto plazo.
- Consultores.
- Auditores, internos y externos.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso[54].

#### *3.2.2.3.3. Controles de acceso lógico*

#### *a.- Procedimientos de conexión de terminales*

La conexión a un sistema informático debe ser diseñada para minimizar la oportunidad de acceso no autorizado. No debe divulgar información acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado. Por lo tanto el sistema no debe:

- desplegar identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión;
- desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder a la computadora;

[54] El convenio de confidencialidad de la información

- no dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión;
- validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta;
- limitar el número de intentos de conexión no exitosos permitidos (de 3 a 5) y considerar:

    - Registrar los intentos no exitosos;
    - Implementar una demora obligatoria antes de permitir otros intentos de identificación, o rechazar otros intentos sin autorización específica;
    - Desconectar la conexión, luego de 3 intentos sucesivos de conexión ;

- Guardar la siguiente información, en un archivo o log, al completarse una conexión exitosa:

    - fechas y hora de la conexión exitosa anterior;
    - detalles de los intentos de conexión no exitosos desde la última conexión exitosa

**b.- Identificación y autenticación de los usuarios**

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo.

Los ID de usuario no deben dar ningún inicio del nivel de privilegio del usuario, p.ej. gerente, supervisor, etc. En circunstancias excepcionales, cuando existe un claro beneficio para la compañía, pueda utilizarse un ID compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se debe documentar la aprobación de la gerencia. Podrían requerirse controles adicionales para mantener la responsabilidad con la firma de actas de riesgo así como documentación adicional en las cuales se deje indicado el nombre de usuario y las personas que están en su uso.

Quedan autorizados los métodos de autenticación automática que permitan el acceso lógico a los sistemas de información así como a sitios físicos restringidos, siempre y cuando permitan el acceso solo al personal autorizado para el acceso y/o uso de sistemas de información. Existen diversos procedimientos de autenticación, los cuales pueden ser utilizados para sustentar la identidad alegada del usuario. También se puede llevar a cabo lo mismo con medios criptográficos y protocolos de autenticación. Los objetos como “tokens” con memoria o tarjetas inteligentes que poseen los usuarios también pueden utilizarse.

Las tecnologías de autenticación biométrica que utilizan las características o atributos únicos de un individuo también pueden utilizarse para autenticar la identidad de una persona. Una combinación de tecnologías y mecanismos vinculados de manera segura tendrá como resultado una autenticación más fuerte, queda a libre disposición de las áreas la utilización de esta posibilidad de autenticación.

**c.- Sistema de administración de contraseñas.**

Los sistemas o módulos de administración de contraseñas de aplicaciones críticas de la organización deben constituir una herramienta eficaz e interactiva que garantice la parametrización de contraseñas según lo establecido en el numeral 3.2.2.3.1.

En las aplicaciones que requieren que las contraseñas de usuario sean asignadas por una autoridad independiente, la aplicación debe forzar a un cambio de

contraseña la próxima vez que el usuario inicie una sesión, además esta contraseña inicial no debe ser fácil de adivinar o conseguir. En los casos que las contraseñas sean seleccionadas y mantenidas por los usuarios es responsabilidad de estos su cuidado.

El sistema o modulo de administración de contraseñas debe:

- imponer el uso de contraseñas individuales para determinar responsabilidades;
- cuando corresponda, permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso;
- imponer una selección de contraseñas de calidad según el numeral 3.2.2.3.1
- cuando los usuarios mantienen sus propias contraseñas, imponer cambios en las mismas según lo señalado en el punto;
- cuando los usuarios seleccionan contraseñas, obligarlos a cambiar las contraseñas temporarias en su primer procedimiento de identificación.;
- mantener un registro de las contraseñas previas del usuario, p.ej. de los 12 meses anteriores, y evitar la reutilización de las mismas;
- no mostrar las contraseñas en pantalla, cuando son ingresadas;
- almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación;
- almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional;
- modificar las contraseñas predeterminadas por el vendedor, una vez instalado el software.

**d.- Desconexión de terminales por tiempo muerto**

Las sesiones de terminales a servicios catalogados como críticos o que sirven a sistemas de alto riesgo, deben terminarse después de un periodo definido de inactividad, para evitar el consumo de recursos así como el de evitar accesos no autorizados. Los administradores de aplicativos en conjunto con los administradores de bases de datos determinarán el tipo de cuentas cuyas sesiones no deben terminarse después de un periodo definido de inactividad. El lapso por tiempo muerto debe responder a las necesidades de conexión de cada usuario.

Así mismo, el administrador del aplicativo así como los administradores de base de datos deben disponer a los usuarios los horarios aprobados de conexión para reducir el espectro de oportunidades para el acceso no autorizado. Se debe considerar un control de esta índole para las aplicaciones críticas y sus elementos de configuración como servidores, bases de datos, y elementos de comunicación. Estos controles deben implementarse especialmente para:

- utilización de lapsos predeterminados, p.ej. para transmisiones de archivos e lote, o sesiones interactivas periódicas de corta duración;
- limitación de los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

### 3.2.2.4. Seguridad Física y Ambiental

#### *3.2.2.4.1. Perímetro de seguridad*

La protección física se llevará a cabo mediante la implementación de barreras físicas y lógicas en los edificios e instalaciones donde se encuentren las instalaciones de procesamiento de datos que se hayan considerados críticos.

Los siguientes lineamientos deben ser seguidos por los jefes de área que tengan bajo su cargo o responsabilidad una instalación de procesamiento de datos crítica:

a. Definir y documentar claramente el perímetro de seguridad.

b. Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican

c. Verificar la existencia de un área de recepción atendida por personal de seguridad que filtre el ingreso de personal no autorizado llevando una bitácora de los ingresos, donde conste el nombre, número de cédula y fecha del ingreso.

d. Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.

e. Identificar claramente todas las puertas de salida de emergencia en un perímetro de seguridad.

f. El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

- Identificación del Edificio y Áreas principales
- Elementos a proteger.
- Medidas de protección física

#### *3.2.2.4.2. Controles de acceso físico a zonas restringidas*

a. Todos los visitantes se registrarán en recepción firmando la entrada y la salida. Los datos mínimos a requerir son: apellido y nombres, tipo y Nº de documento presentado, compañía a la que pertenece, empleado de referencia, motivo de la visita, hora de entrada y salida. El empleado organizador de la visita debe recibir al visitante en su oficina y desde allí lo acompañará al área restringida.

b. La entrada de cualquier persona al centro de cómputo fuera del horario habitual de trabajo, deberá estar autorizada formalmente y registrada en la bitácora o planilla de ingresos.

c. El responsable del centro de cómputo (CDC) es el encargado primario del control y seguimiento de los registros de accesos, y deberá actuar en consecuencia ante sospechas de violaciones de la misma.
d. Todos los servidores o equipos centrales, y las consolas de operación, que integran el ámbito de procesamiento deberán residir dentro del centro de cómputo.
e. En el CDC la entrada debe estar protegida apropiadamente contra accesos no autorizados (por ej.: cerraduras, mecanismos de control, alarmas, etc.) y su señalización debe ser la mínima indispensable, a fin de evitar la identificación de actividades en esa área.
f. Las tareas de limpieza en el centro de cómputo será supervisada por una persona responsable de la sala que pueda advertir y evitar incidentes accidentales o intencionales sobre los equipos.

**Para acceder al centro de cómputo en horarios de oficina (08:00 a 16:30)**

g. Para que el personal de la Gerencia Nacional de TI, puedan acceder al CDC a realizar tareas de mantenimiento, administración y/o tareas de su competencia, deberán llenar la solicitud de acceso al centro de cómputo y contar con la aprobación del Responsable del CDC.
h. Personal de las áreas de Redes y Servidores pueden ingresar al CDC con la autorización del Responsable del CDC, para ello deben llenar la solicitud de acceso al centro de cómputo.
i. Personas ajenas a la CNT S.A. y las áreas de Redes y Servidores que requieran acceso al CDC, deberán primero contactar con su respectiva contraparte técnica dentro de la Gerencia Nacional de TI y serán estos quienes soliciten el respectivo permiso para ingresar al CDC, para ello deberán llenar la solicitud de acceso al centro de cómputo y contar con la aprobación del Responsable del CDC.
j. Personal ajeno La CNT S.A. debe estar acompañada durante todo el tiempo que dure la visita, por personal de la Gerencia Nacional de TI.

k. Toda persona debe llenar la respectiva bitácora de acceso al CDC, esto incluye al propio personal del CDC.

**Para acceder al centro de cómputo en horarios fuera de oficina (16:30 a 08:00)**

l. Para que personal de las áreas de Servidores y Redes pueda acceder a las instalaciones del centro de cómputo en horarios fuera de oficina, estos deberán programar sus visitas con anterioridad y entregar la solicitud de acceso al centro de cómputo antes de las 16:30, para que el responsable del CDC informe al operador de turno sobre los accesos programados. Caso contrario no podrán ingresar

m. Para que personas ajenas a la CNT S.A. y a las áreas de Redes y Servidores puedan acceder al centro de cómputo en horarios fuera de oficina, deberán programar sus visitas y presentar el respectiva formato de solicitud de acceso al centro de cómputo la misma que deberá ser llenada por personal de la Gerencia Nacional de TI que será responsable de su ingreso y lo supervisará y acompañará durante todo el tiempo que dure su visita. De esta manera el Responsable del Centro de Cómputo podrá informar al operador de turno sobre los accesos programados. Caso contrario no podrán ingresar.

**Para casos de emergencia (casos excepcionales donde la operatividad de los servicios críticos de la organización estuviera en riesgo de una paralización total)**

**En horarios de oficina (08:00 a 16:30)**

n. Si la emergencia se presenta en horarios de oficina, el Responsable del CDC estará en la capacidad de otorgar el acceso inmediatamente de forma verbal (ya sea de forma directa o por medios telefónicos). Luego de subsanado el inconveniente que dio lugar a la emergencia, es

obligación del Responsable del CDC llenar completamente el formato de solicitud de acceso al centro de cómputo.

o. Sí existiere un caso de emergencia en horarios de oficina, y por motivos de fuerza mayor no fuera posible contactarse con el Responsable del Centro de Cómputo, es necesario que el operador pida autorización al Gerente de Soporte Informático de manera verbal. De no encontrarse disponible el/la Gerente de Soporte Informático, la autorización deberá provenir de la Gerencia Nacional de TI. Luego de subsanado el inconveniente que dio lugar a la emergencia, es obligación del Responsable del CDC llenar completamente el formato de solicitud de acceso al centro de cómputo y formalizar el acceso.

**En horarios fuera de oficina (16:30 a 08:00)**

p. Sí existiere un caso de emergencia fuera de horarios de oficina, es necesario que el operador de turno pida autorización de manera verbal al Responsable del CDC. El Responsable del Centro de Cómputo luego de la emergencia regularizará el acceso autorizado mencionando los motivos y causas del mencionado acceso.

q. De no encontrarse disponible el Responsable del CDC, la autorización deberá venir por parte de la Gerencia de Soporte Informático, y de no encontrarse disponible el/la Gerente de Soporte Informático, la autorización deberá provenir de la Gerencia Nacional de TI. Luego de subsanado el inconveniente que dio lugar a la emergencia, es obligación del Responsable del CDC llenar completamente el formato de solicitud de acceso al centro de cómputo y formalizar el acceso.

**Toda persona que ingrese al CDC debe llenar la respectiva bitácora de acceso al CDC, esto incluye al propio personal de la mencionada área.**

### 3.2.2.5. Seguridad en la Red

#### *3.2.2.5.1 Red cableada e inalámbrica y uso de sus recursos.*

Los recursos de red son recursos que se agotan, como los recursos financieros. Es por tanto que los empleados deben cuidar que estos recursos no se agoten con la finalidad que la comunicación en la compañía no sufra de retardos que se vean reflejados en la baja de producción.

.

El Área de redes deberá velar porque los recursos de la red no sean consumidos de una manera irresponsable por los usuarios, y deberá establecer las mejores configuraciones de los equipos, con relación a seguridad y eficiencia, de manera que la red este siempre en operación.

El Responsable de Redes será el encargado de llevar un diagrama con el perímetro lógico de las redes de la compañía, donde consten los dispositivos que representen barreras para los intrusos internos o externos, así como de las reglas configuradas en cada uno de ellos:

a. Firewall
b. IPS
c. Firewall en las PC´s (definido sobre el inventario de software que el Área de PC´s debe llevar).

Todos los equipos de usuario que se conecten a la red corporativa de datos para utilizar los servicios de correo electrónico, Internet, intranet, sistemas transaccionales y/o se destinen para realizar las actividades de operación, mantenimiento y gestión de centrales telefónicas o equipos de las redes de servicio público de La CNT S.A., deben ser ingresados al dominio de la CNT S.A.

Los equipos que no se encuentren bajo la responsabilidad y administración directa de la Gerencia Nacional de TI deberán estar en subredes específicas. En

coordinación con el área de redes se analizará y controlará con cuales redes se pueden interactuar.

El responsable y/o administrador del área observará que lo adquirido (software y/o hardware), cumpla con las características de compatibilidad de infraestructura y software administrado por la Gerencia Nacional de TI, debe garantizar el correcto funcionamiento de las aplicaciones, el soporte, mantenimiento, evitar daños por no compatibilidad, virus y debilidades en acceso a los datos de la compañía.

Previo a todo cambio que se aplique en la red, equipos de comunicación y/o dispositivos, deberá ser analizado en función de medir el riesgo e impacto que este cambio pueda presentar a los servicios, en el caso que este cambio tenga relación o afectación sobre la red interna de la CNT S.A..., deberá coordinarse con la Gerencia Nacional de TI.

El responsable del área que tenga a cargo o bajo su administración red, equipos, deberá mantener al día aplicados los parches y actualizaciones recomendadas por el fabricante.

Está prohibida la utilización de cuentas y contraseñas que vienen configuradas por defecto en los equipos de interconectividad de la red.

#### *3.2.2.5.2. Seguridad en la red inalámbrica*

La red inalámbrica debe estar separada de la red de usuarios internos de la compañía, y no una extensión de la misma, con ingreso limitado a los servidores y recursos de red. Debe contar con mecanismos de autenticación y autorización de usuarios registrados para lo cual debe contar con sistemas propietarios o abiertos que garanticen el no ingreso de usuarios no autorizados.

Se debe implementar tipos de encripción como LEAP o WPA2 como sistemas de autenticación y cifrado de datos y el filtrado mediante listas de control de acceso o sistemas de firewall de los recursos disponibles en la red corporativa de datos.

El acceso inalámbrico (Wireless) es autorizado por defecto a todos los jefes de área e inmediatos superiores que se encuentren debidamente registrados dentro del organigrama organizacional.

El área de infraestructura garantizará la entrega de los equipos portátiles, con las opciones Bluetooth, Wireless, dispositivos infrarrojos y módems deshabilitadas. Solo los usuarios con autorización de acceso Wireless podrán tener habilitada la mencionada opción.

Los puntos de acceso inalámbrico no pueden ser adquiridos o instalados de manera indiscriminada por usuarios y/o áreas diferentes a la de infraestructura. En caso de necesidad de instalación y/o ampliación, se debe solicitar el soporte respectivo a la Gerencia Nacional de TI.

En caso de necesitar una red inalámbrica ajena a la red de cobertura general, por ejemplo un laboratorio de pruebas, esta se deberá instalar de forma autónoma e independiente, totalmente desconectada de la red corporativa, respetando en todos los casos el espectro electromagnético de la red inalámbrica ya existente y con autorización previa de la Gerencia de Producción de TI.

El área de Infraestructura debe asegurar:

a. La existencia de un sistema de autenticación y de autorización que no permita el acceso de usuarios a la red inalámbrica sin que estos no estén previamente validados.

b. La implementación de un esquema de cifrado de información que no permita en un corto periodo de tiempo (menor a 5 horas) criptoanalizar el tráfico inalámbrico de manera que comprometa la integridad y confidencialidad de la información transmitida.
c. La existencia de un plan de actualización de firmware de todos los puntos de acceso inalámbrico (Access Point).
d. Está prohibido tener los nombres de red (SSID) que vienen configurados por default en los puntos de acceso, de igual manera inhabilitar la emisión broadcast del nombre de red (SSID).
e. Se debe reducir al mínimo la cobertura del alcance de la señal de los puntos de acceso inalámbricos, limitándoles únicamente al edificio donde reside la red.

#### 3.2.2.6. Seguridad de bases de datos, servidores, redes, lineamientos para los administradores

a. Los lineamientos de seguridad son desarrollados por el área de seguridad informática, y su implementación es responsabilidad de los administradores y bajo ningún motivo se podrá revelar su configuración y esquemas de funcionamiento. La documentación resultante de las configuraciones de seguridad implementadas deberán poseer características que impidan su difusión no autorizada.
b. Los administradores son responsables del diseño, definición, funcionamiento y mantenimiento, además del manejo de recursos de los cuales depende la disponibilidad, integridad y confidencialidad de la información contenida en esta.
c. Los súper-usuarios de Sistemas de Información y/o Aplicativos que requieren acceso a las Bases de Datos, servidores y/o equipos de comunicación, solo podrán ser solicitados por el Gerente Nacional,

Gerentes Regionales, Gerentes, y previa validación del Área de Seguridad Informática estos podrán serán creados.

d. Los administradores en casos donde la disponibilidad, integridad o confidencialidad de la información pueda comprometerse, podrán eliminar procesos de usuarios que directamente estén afectando estos parámetros.
e. Los Administradores establecerán mecanismos de seguridad para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
f. Los Administradores deberán prever el mejor esquema de licenciamiento en costo y funcionalidad para cada uno de los sistemas que administra.
g. La información que previamente haya sido catalogada como confidencial y se encuentre almacenada en las bases de datos de la institución, deberá ser cifrada con un algoritmo que previa validación por parte del área de seguridad informática, será implementada por los administradores.
h. Los administradores deben garantizar que las cuentas y contraseñas configuradas en sus sistemas por defecto o de fábrica no se utilicen.
i. Los administradores deben garantizar la instalación de parches y actualizaciones remitidas por el fabricante.
j. Los administradores deben utilizar protocolos seguros para la gestión remota del equipo.
k. Los administradores deben deshabilitar servicios no necesarios para el correcto funcionamiento de los componentes o servicios que soporta el sistema.
l. Todos los equipos deben tener una referencia horaria común, responsabilidad de su parametrización el área de redes y servidores.
m. Los administradores deben almacenarse localmente en los equipos y en un servidor dispuesto para el efecto.

#### *3.2.2.6.1. Respaldos de información*

n. El Administrador de la base de datos y el jefe del área del centro de cómputo (donde aplique) son responsables de los respaldos cuyas características se hayan definido en conjunto con el administrador de la aplicación en acta debidamente formalizada, El administrador de la aplicación está en la facultad de probar los respaldos de su aplicativo previa coordinación con las áreas pertinentes, donde se verifique lo acordado.

o. Los administradores de aplicativos deberán entregar a los administradores de base de datos los procedimientos de respaldos y recuperación de datos. Esto aplica en los casos en que los procedimientos de respaldos y recuperación propios de la administración de base de datos sean atípicos a los comúnmente realizados o dependan de cierto tipo de actividades secuenciales y especiales.

p. El administrador de base de datos, debe planificar una vez, cada seis meses, el reinicio completo de las base de datos.

q. Los administradores son responsables de realizar un respaldo inicial de los archivos de configuración y datos necesarios para la normal operación de sus sistemas.

r. Los administradores deben definir y establecer los mecanismos de recuperación en caso de presentarse alguna situación que provoque la pérdida de acceso a la información almacenada y falta de disponibilidad del servicio que soportan.

#### *3.2.2.6.2. Mantenimientos de Equipos*

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, se debe considerar:

s. Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con intervalos de servicio y especificaciones recomendados por el proveedor o fabricante.

t. Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo correctivo realizado.

u. Eliminar la información confidencial que contenga cualquier equipo que es necesario retirar (p.ej. PC´s, Flash, disquetes), realizándose previamente las respectivas copias de resguardo.

v. La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

#### *3.2.2.6.3. Seguridad ambiental de equipos*

Con la finalidad de salvaguardar la integridad de los equipos y de asegurar que se evite: negación del servicio y/e interrupción de las actividades del negocio, los administradores deben seguir los siguientes lineamientos:

w. El equipamiento debe ser situado de acuerdo a las especificaciones de la compañía que lo ha manufacturado y de acuerdo a lo especificado en los contratos de garantía, si es que se tienen, con las empresas contratistas.

x. Los equipos en los que se encuentre información identificada como crítica y los equipos que no tuvieren información importante pero que sean críticos en si para el funcionamiento de la CNT S.A. (routers, switches…) deben poseer controles ambientales que los monitoreen y alarmas que se disparen cuando estos controles sobrepasan los límites establecidos por los fabricantes como óptimos para el funcionamiento del equipo.

y. Comer tomar o fumar no está permitido en las áreas donde residan estos equipos, al igual que su ingreso estará restringido y será de responsabilidad del dueño de la información y/o del Responsable del

Área velar para que el control de acceso físico se cumpla (ver numeral 3.3.2.4).

### 3.2.2.7. Seguridad en el sitio de trabajo

Con la finalidad de proteger los documentos en papel y dispositivos de almacenamiento removibles, y en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo se debe seguir las siguientes directrices:

a. Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados (p.ej. cuando vamos a almorzar, reuniones…) especialmente fuera del horario de trabajo.
b. Guardar bajo llave la información que haya sido catalogada como sensible o crítica (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
c. Desconectar de la red y/o sistema y/o servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos debidamente de accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos.

d. Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
e. Cuando se ejecuten impresiones que sean criticas y en las que se utiliza una impresora compartida para toda la oficina, se deben tomar las medidas adecuadas para proteger el documento que ha sido enviado a imprimir por ejemplo:

- Verificar que exista papel en la copiadora.
- No imprimir un documento más veces de lo que se requiera.
- Retirar inmediatamente la información confidencial que fue enviada a imprimir.

f. Para las personas que trabajen con información catalogada como crítica o sensible para la CNT S.A. se les prohíbe:

- Sacar copias de los documentos, salvo previa autorización del dueño de los datos y siempre y cuando se asegure la confidencialidad.
- Divulgar el contenido de la información crítica o sensible o confidencial por cualquier medio.

#### 3.2.2.8. Seguridad de software

##### *3.2.2.8.1. Software no autorizado*

Todas las PC´s de la compañía ya sean de escritorio o portátiles, deben tener software que por defecto el departamento de PC´s ha instalado, y dependiendo de los requerimientos para los cuales el usuario ha sido designado. Los usuarios no están autorizados para la instalación de software en los equipos que la CNT S.A. les haya designado a través del área de PC´s.

Todos los usuarios que dispongan de una PC deben seguir los siguientes lineamientos:

a. El área de Seguridad Informática en conjunto con el área de PC´s serán las encargadas de aprobar la instalación de software nuevo previo a un análisis de riesgos. Esto incluye freeware, shareware, donationware[55], entre otros.
b. Está prohibido la instalación y/o ejecución de software no autorizado en las PC´s propiedad de la CNT S.A. (Ver ley de propiedad intelectual).
c. En el caso de que un visitante de la compañía con su portátil conecte su equipo a la red, se deberá realizar una auditoría del software que posee, al mismo tiempo que se verifique la no existencia de virus. Esto busca disminuir riesgos con respecto a:

    - Ejecución de software para motivos de hacking y de alguna manera comprometer la información en nuestros sistemas.
    - Posible infección de virus o gusanos en la red de la CNT S.A. con o sin intención del personal.

d. El Área de PC´s será la encargada de realizar revisiones periódicas buscando la instalación de software no autorizado debiendo informar al Área de Seguridad Informática y desinstalando el Software de manera inmediata.

***3.2.2.8.2. Virus y gusanos***

Para reducir el riesgo de infección de software malicioso en la red de telecomunicaciones.

[55] Freeware: software gratuito que es distribuido principalmente por internet; shareware software que tiene un periodo de caducidad luego del cual hay que pagar licencia. Donationware: software que es licenciado pero que debido a donaciones su licencia es gratuita para el donado.

a. No abrir mensajes de correo electrónico o archivos no solicitados o sospechosos, que tengan como remitente alguna persona o entidad no conocida.

b. No abrir archivos que se encuentren en cualquiera de los medios extraíbles (CD ROM, disquete, memoria flash) sin antes, no haber realizado un escaneo con el antivirus instalado en su máquina.

c. No instalar en su PC ningún tipo de programa, ya sea gratuito o no y de ninguna manera instalar programas que posean algún tipo de crack56(ver ley de propiedad intelectual).

d. No difundir virus por cualquier medio que trabaje en red (correo electrónico, Messenger, carpetas compartidas…).

e. Borrar inmediatamente y no reproducir cadenas de correo electrónico (spam).

f. Al bajar archivos, desde el Internet, correr el antivirus antes de abrirlo

g. Para el caso de los usuarios de Messenger, no abrir ningún link sospechoso que aparezca en su pantalla de MSN, ni descargar archivos por medio utilizando esta herramienta.

h. Si los usuarios creen ser víctimas de algún virus/gusano o haber abierto algún archivo que contenga el virus/gusano debe ponerse en contacto lo más pronto posible con el departamento de PC´s

#### 3.2.2.9. Comunicación sobre incidentes y brechas de seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Área de Seguridad Informática inmediatamente luego de conocerlas para evitar cualquier incidente de seguridad.

[56] Programa que realiza una modificación permanente o temporal sobre otro o en su código, para obviar una limitación o candado impuesto a propósito por el programador original. Este tipo de programas ilegales facilita la vulneración de los derechos de autor.

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

Igualmente los usuarios al enterarse de la existencia en sus computadores, en los computadores de los compañeros de trabajo, o en algún archivo que este circulando por la red (p.ej. correo electrónico) que contenga código malicioso, virus, gusanos deberá contactarse con el Área de Seguridad Informática, Desk-Desk y/o con el Área de PC´s.

El Área de Desk-Desk deberá informar acerca de cualquier brecha de seguridad que tengan conocimiento, al igual que informar sobre cualquier incidente de seguridad a Área de Seguridad Informática.

Para el escalamiento de problemas y solución de los mismos referirse al procedimiento ¨ Gestión de incidentes y problemas ¨ del área de Desk-Desk.

#### 3.2.2.10. Sanciones

El área de seguridad informática una vez conocido el incidente de seguridad realizará un informe de lo acontecido, que será validado por el gerente de área, previo la recopilación de información en el/los sistema(s) afectados. Este informe será enviado al área de recursos humano quienes serán los encargados de emitir las sanciones correspondientes acorde al reglamento interno, y tomando en cuenta además las leyes del Ecuador con relación a la infracción cometida.

#### 3.2.2.11. Referencias a la ley

##### *3.2.2.11.1. Correo Electrónico, Firmas Y Mensajes De Datos*

**Comentario:** el extracto de esta ley define a las infracciones informáticas sobre información protegida que son motivo de algún tipo de sanción pecuniaria y/o de privación de la libertad en el estado ecuatoriano. Todas las leyes abajo recopiladas son adiciones al código penal e incluyen multas y prisión desde 500 dólares y seis

meses de prisión hasta los nueve años y multas que ascienden hasta los 10.000 USD. La pena es agravada si las infracciones informáticas se cometen sobre información que está relacionada con la seguridad nacional. Las infracciones informáticas tratan el acceso no autorizado a información protegida, la apropiación ilícita y la mala utilización de la misma tomando en cuenta los intereses del perjudicado. Hay que poner un especial énfasis en el artículo 262 relacionado estrechamente con los trabajadores del sector público y los delitos que contra la información protegida son motivo de sanción.

**…**

**Art. 5.- Confidencialidad y reserva.-** Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

**Art. 9.- Protección de datos.-** Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

**TITULO V**
**DE LAS INFRACCIONES INFORMÁTICAS**
**CAPITULO I**
**DE LAS INFRACCIONES INFORMÁTICAS**

**Art. 57.- Infracciones informáticas.-** Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

**Reformas al Código Penal**

**Art. 58.-** A continuación del artículo202, inclúyanse los siguientes artículos Enumerados:

"Art...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

**Art. 59.- Sustitúyase el artículo 262 por el siguiente:**

**"Art. ...- 262.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

**Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:**

"**Art. ...- Falsificación electrónica.-** Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho. El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.".

**Art. 61.- A continuación del artículo415 del Código Penal, inclúyanse los siguientes artículos innumerados:**

**"Art. ...- Daños informáticos.-** El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

**Art. ...-** Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.".

**Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados**:

"**Art. ...- Apropiación ilícita.-** Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

**Art. ...-** La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

**Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:**

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

**Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:**

"... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos."

#### *3.2.2.11.2. Ley de propiedad intelectual*

**Comentario**: el extracto de esta ley permite imponer sanciones sobre delitos cometidos a la propiedad intelectual perteneciente a la compañía. Entiéndase como “obra” al producto intelectual de los trabajadores que en cumplimiento de los objetivos impuestos por la compañía y en función de las responsabilidades encomendadas por la misma se han desarrollado. Así por ejemplo tenemos como “obras” el desarrollo de software interno o mejoramiento del mismo, desarrollo de

manuales de implementación tecnológica, reglamentos internos entre otros. La difusión de estas obras, su alteración y copias sin consentimiento del titular son en general los delitos que son sancionados en esta ley.

CONSTITUCIÓN POLÍTICA DE LA REPUBLICA DEL ECUADOR: Arts. 23 (Inc. 23).

**Art. 20.- El derecho exclusivo de explotación de la obra comprende especialmente la facultad de realizar, autorizar o prohibir:**

**a)** La reproducción de la obra por cualquier forma o procedimiento;
**b)** La comunicación pública de la obra por cualquier medio que sirva para difundir las palabras, los signos, los sonidos o las imágenes;
**c)** La distribución pública de ejemplares o copias de la obra mediante la venta, arrendamiento o alquiler;
**d)** La importación; y,
**e)** La traducción, adaptación, arreglo u otra transformación de la obra.

La explotación de la obra por cualquier forma, y especialmente mediante cualquiera de los actos enumerados en este artículo es ilícita sin la autorización expresa del titular de los derechos de autor, salvo las excepciones previstas en esta Ley.

**Art. 21.-** La reproducción consiste en la fijación o réplica de la obra en cualquier medio o por cualquier procedimiento, conocido o por conocerse, incluyendo su almacenamiento digital, temporal o definitivo, de modo que permita su percepción, comunicación o la obtención de copias de toda o parte de ella.

**Art. 22.-** Se entiende por comunicación pública todo acto en virtud del cual una pluralidad de personas, reunidas o no en un mismo lugar y, en el momento en que individualmente decidan, puedan tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas, como en los siguientes casos:

**a)** Las representaciones escénicas, recitales, disertaciones y ejecuciones públicas de las obras dramáticas, dramático - musicales, literarias y musicales, mediante cualquier medio o procedimiento;
**b)** La proyección o exhibición pública de las obras cinematográficas y de las demás obras audiovisuales;
**c)** La radiodifusión o comunicación al público de cualesquiera obras por cualquier medio que sirva para difundir, sin hilo, los signos, los sonidos o las imágenes, o la representación digital de éstos, sea o no simultánea.

La transmisión de señales codificadas portadoras de programas es también un acto de comunicación pública, siempre que se ponga a disposición del público por la entidad radiodifusora, o con su consentimiento, medios de decodificación.

A efectos de lo dispuesto en los dos incisos anteriores, se entenderá por satélite cualquiera que opere en bandas de frecuencia reservadas por la legislación de telecomunicaciones a la difusión de señales para la recepción por el público o para la comunicación individual no pública, siempre que en este último caso las circunstancias en que se lleve a efecto la recepción individual de las señales sean comparables a las que se aplican en el primer caso;

**d)** La transmisión al público de obras por hilo, cable, fibra óptica u otro procedimiento análogo, sea o no mediante abono;
**e)** La retransmisión de la obra radiodifundida por radio, televisión, o cualquier otro medio, con o sin hilo, cuando se efectúe por una entidad distinta de la de origen;
**f)** La emisión, transmisión o captación, en lugar accesible al público, mediante cualquier instrumento idóneo de la obra radiodifundida;
**g)** La presentación y exposición públicas;

**h)** El acceso público a bases de datos de ordenador por medio de telecomunicación, cuando estas incorporen o constituyan obras protegidas; e,

**i)** En fin, la difusión por cualquier procedimiento conocido o por conocerse, de los signos, las palabras, los sonidos, las imágenes de su representación, u otras formas de expresión de las obras. Se considerará pública toda comunicación que exceda el ámbito estrictamente doméstico.

**Art. 26.-** También constituyen violación de los derechos establecidos en este libro cualquiera de los siguientes actos:

**a)** Remover o alterar, sin la autorización correspondiente, información electrónica sobre el régimen de derechos; y,

**b)** Distribuir, importar o comunicar al público el original o copias de la obra sabiendo que la información electrónica sobre el régimen de derechos ha sido removida o alterada sin autorización;

Se entenderá por información electrónica aquella incluida en las copias de obras, o que aparece en relación con una comunicación al público de una obra, que identifica la obra, el autor, los titulares de cualquier derecho de autor o conexo, o la información acerca de los términos y condiciones de utilización de la obra, así como número y códigos que representan dicha información.

**Art. 183.-** Se protege la información no divulgada relacionada con los secretos comerciales, industriales o cualquier otro tipo de información confidencial contra su adquisición, utilización o divulgación no autorizada del titular, en la medida que:

**a)** La información sea secreta en el entendido de que como conjunto o en la configuración y composición precisas de sus elementos no sea conocida en general ni fácilmente accesible a las personas integrantes

de los círculos que normalmente manejan el tipo de información de que se trate;

**b)** La información tenga un valor comercial, efectivo o potencial, por ser secreta; y,

**c)** En las circunstancias dadas, la persona que legalmente la tenga bajo control haya adoptado medidas razonables para mantenerla secreta.

La información no divulgada puede referirse, en especial, a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o, a los medios o formas de distribución o comercialización de productos o prestación de servicios.

También son susceptibles de protección como información no divulgada el conocimiento tecnológico integrado por procedimientos de fabricación y producción en general; y, el conocimiento relativo al empleo y aplicación de técnicas industriales resultantes del conocimiento, experiencia o habilidad intelectual, que guarde una persona con carácter confidencial y que le permita mantener u obtener una ventaja competitiva o económica frente a terceros.

Se considera titular para los efectos de este Capítulo, a la persona natural o jurídica que tenga el control legítimo de la información no divulgada.

**Art. 184.-** El titular podrá ejercer las acciones que se establecen en esta Ley para impedir que la información no divulgada sea hecha pública, adquirida o utilizada por terceros; para hacer cesar los actos que conduzcan en forma actual o inminente a tal divulgación, adquisición o uso; y, para obtener las indemnizaciones que correspondan por dicha divulgación, adquisición o utilización no autorizada.

**Art. 185.-** Sin perjuicio de otros medios contrarios a los usos o prácticas honestas, la divulgación, adquisición o uso de información no divulgada en forma contraria a esta Ley podrá resultar, en particular, de:

**a)** El espionaje industrial o comercial;

**b)** El incumplimiento de una obligación contractual o legal;

**c)** El abuso de confianza;

**d)** La inducción a cometer cualquiera de los actos mencionados en los literales a), b) y c); y,

**e)** La adquisición de información no divulgada por un tercero que supiera, o que no supiera por negligencia, que la adquisición implicaba uno de los actos mencionados en los literales a), b), c) y d).

**Art. 186.-** Serán responsables por la divulgación, adquisición o utilización no autorizada de información no divulgada en forma contraria a los usos y prácticas honestos y legales, no solamente quienes directamente las realicen, sino también quien obtenga beneficios de tales actos o prácticas.

**Art. 190.-** Toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información no divulgada, deberá abstenerse de usarla y de divulgarla, sin causa justificada, calificada por el juez competente y sin consentimiento del titular, aún cuando su relación laboral, desempeño de su profesión o relación de negocios haya cesado.

#### *3.2.2.11.3. Ley de transparencia y acceso a la información pública*

**Comentario:** Esta ley dictamina la necesidad de clasificación de información en las entidades del sector público. Esta clasificación estará en función de los intereses nacionales y de los intereses u objetivos estratégicos de la compañía. Como se menciona en la ley se debe realizar un inventario de información confidencial la cual estará clasificada como tal un periodo de quince años. El resto de información estará disponible para el que requiera su acceso mediante un portal aunque su acceso

puede ser solicitado por medio escrito, la denegación de este acceso, su falta de veracidad o de su totalidad deviene en sanciones.

**Art. 6.- Información Confidencial.-**

Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales,

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.

No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

**Art. 13.- Falta de claridad en la Información.-**

Cuando se demuestre por parte de cualquier ciudadano, que existe ambigüedad en el manejo de la información, expresada en los portales informáticos, o en la información que se difunde en la propia institución, podrá exigirse personalmente la corrección en la difusión, de no hacerlo podrá solicitarse la intervención del Defensor del Pueblo a efectos de que se corrija y se brinde mayor claridad y sistematización, en la organización de esta información.

El Defensor del Pueblo, dictaminará los correctivos necesarios de aplicación obligatoria a la información que se difunde; al efecto, la institución brindará las facilidades amplias y suficientes, so pena de destitución, previo sumario

administrativo, de las autoridades que incumplan su obligación de difundir la información institucional correctamente. La sanción dictaminada por el Defensor del Pueblo, será ejecutada inmediatamente por la autoridad nominadora.

**Art. 18.- Protección de la Información Reservada.-**

La información clasificada previamente como reservada, permanecerá con tal carácter hasta un período de quince años desde su clasificación. La información reservada será desclasificada cuando se extingan las causas que dieron lugar a su clasificación. Se ampliará el período de reserva sobre cierta documentación siempre y cuando permanezcan y se justifiquen las causas que dieron origen a su clasificación.

El Consejo de Seguridad Nacional, en los casos de reserva por motivos de seguridad nacional y los titulares de las instituciones públicas, será responsable de clasificar y desclasificar la información de conformidad con esta Ley. La clasificación de reserva no podrá efectuarse posteriormente a la solicitud de información.

La información reservada que se haga pública antes del vencimiento del plazo de la reserva o de manera distinta a la prevista en el inciso anterior, podrá ocasionar responsabilidad civil, administrativa y/o penal según los casos, de la persona que por su función haya violado la reserva.

Las instituciones públicas elaborarán semestralmente por temas, un índice de los expedientes clasificados como reservados. En ningún caso el índice será considerado como información reservada. Este índice de información reservada, detallará: fecha de resolución y período de vigencia de esta clasificación.

La información reservada en temas de seguridad nacional, solo podrá ser desclasificada por el Consejo de Seguridad Nacional. La información clasificada

como reservada por los titulares de las entidades e instituciones del sector público, podrá ser desclasificada en cualquier momento por el Congreso Nacional, con el voto favorable de la mayoría absoluta de sus integrantes, en sesión reservada.

**Titulo Sexto: De las Sanciones**

**Art. 23.- Sanción a funcionarios y/o empleados públicos y privados.-**

Los funcionarios de las entidades de la Administración Pública y demás entes señalados en el artículo 1 de la presente Ley, que incurrieren en actos u omisiones de denegación ilegítima de acceso a la información pública, entendiéndose ésta como información que ha sido negada total o parcialmente ya sea por información incompleta, alterada o falsa que proporcionaron o debieron haber proporcionado, serán sancionados, según la gravedad de la falta, y sin perjuicio de las acciones civiles y penales a que hubiere lugar, de la siguiente manera:

**a)** Multa equivalente a la remuneración de un mes de sueldo o salario que se halle percibiendo a la fecha de la sanción;
**b)** Suspensión de sus funciones por el tiempo de treinta días calendario, sin derecho a sueldo o remuneración por ese mismo lapso; y,
**c)** Destitución del cargo en caso de que, a pesar de la multa o suspensión impuesta, se persistiere en la negativa a la entrega de la información.

Estas sanciones serán impuestas por las respectivas autoridades o entes nominadores.

Los representantes legales de las personas jurídicas de derecho privado o las naturales poseedoras de información pública que impidan o se nieguen a cumplir con las resoluciones judiciales a este respecto, serán sancionadas con una multa de cien a quinientos dólares por cada día de incumplimiento a la resolución, que será

liquidada por el juez competente y consignada en su despacho por el sancionado, sin perjuicio de las responsabilidades civiles o penales a que hubiere lugar.

Las sanciones se impondrán una vez concluido el respectivo recurso de acceso a la información pública establecido en el artículo 22 de la presente Ley.

La remoción de la autoridad, o del funcionario que incumpliere la resolución, no exime a quien lo reemplace del cumplimiento inmediato de tal resolución bajo la prevención determinada en este artículo.

### 3.2.3. PROCEDIMIENTOS Y LINEAMIENTOS

Se desarrollará lo siguiente:

- Procedimiento de creación modificación y eliminación de cuentas de usuario
- Lineamientos para el establecimiento del proceso de manejo de incidentes.
- Guía para la clasificación de información en procesos críticos.

## DESARROLLO

#### 3.2.3.1. Procedimiento de creación modificación y eliminación de cuentas de usuario.

**Objetivo:**

Normar la creación eliminación y modificación de usuarios en los sistemas de la CNT S.A.

**Alcance:**

Este procedimiento abarca la totalidad de los usuarios que necesitan ingresar a los sistemas de la CNT S.A.

El procedimiento actual se encuentra esquematizado en la figura 3.1 en ella se puede apreciar cual es el tiempo estimado que toma el proceso de creación y modificación de usuarios, alrededor de 3 a 4 días, con la problemática de accesos antes mencionada. El proceso propuesto(ver figura 3.2) disminuye los tiempos de atención y aumenta los niveles de seguridad de la empresa. Este procedimiento tiene un prerrequisito: El levantamiento de información de los perfiles con relación a los cargos dentro de la institución con la finalidad de poseer los permisos que cada trabajador necesita para realizar sus funciones. Cualquier permiso extra que se requiera nace desde el usuario pero es aprobado por el administrador del aplicativo.

## PROCEDIMIENTO ACTUAL DE CREACIÓN O MODIFICACIÓN DE USUARIOS

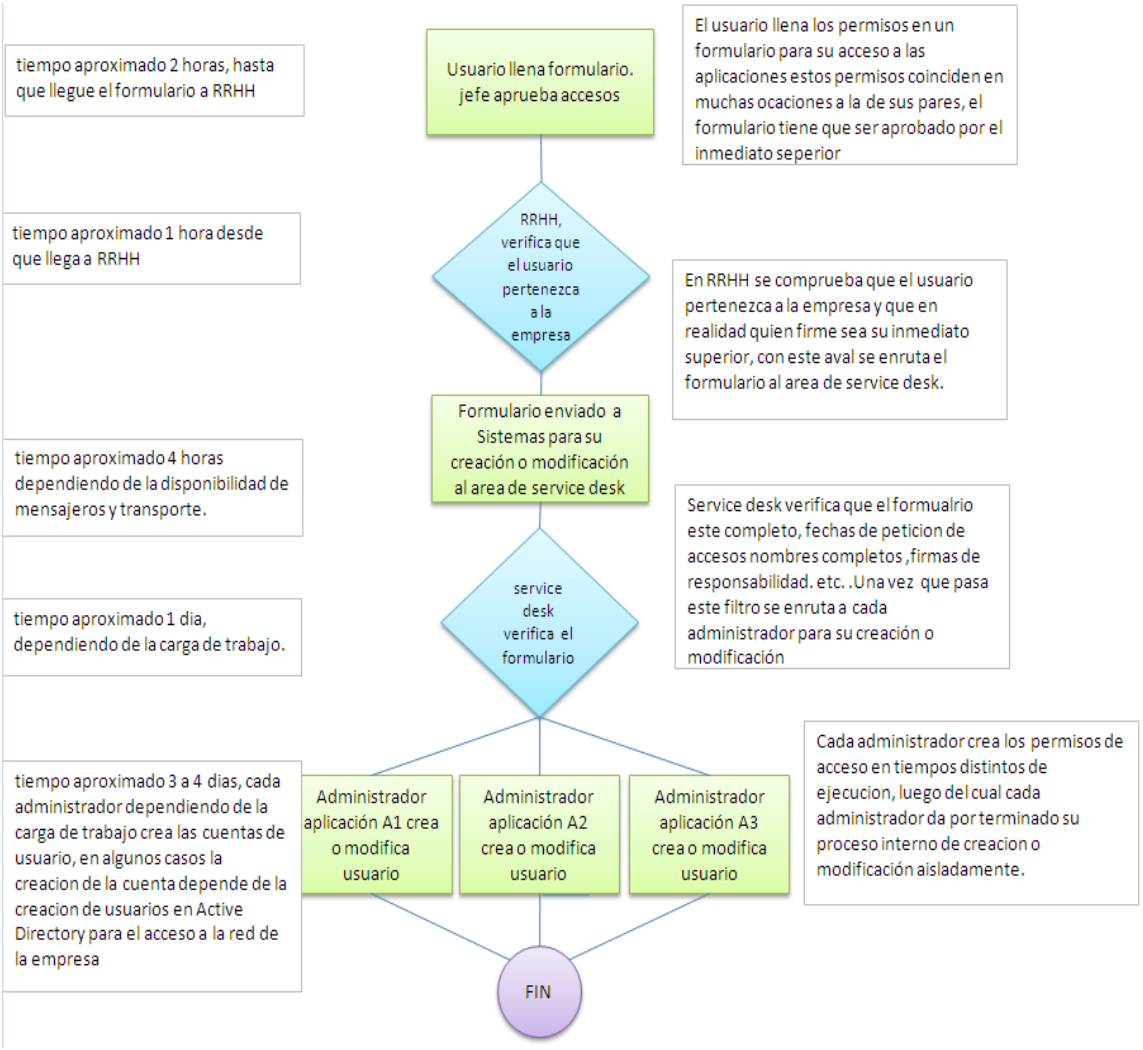



FIG 3.1 Procedimiento actual de modificación de cuentas de usuario

Para el caso de eliminación de cuentas el pedido se lo hace telefónicamente o por medio de correo electrónico a los administradores de las aplicaciones, principalmente de active directory (red y correo electrónico) y la eliminación se la realiza de manera aislada, aumentando de manera significativa el tiempo de ejecución de este proceso

## PROCEDIMIENTO PROPUESTO PARA LA CREACIÓN O MODIFICACIÓN DE USUARIOS

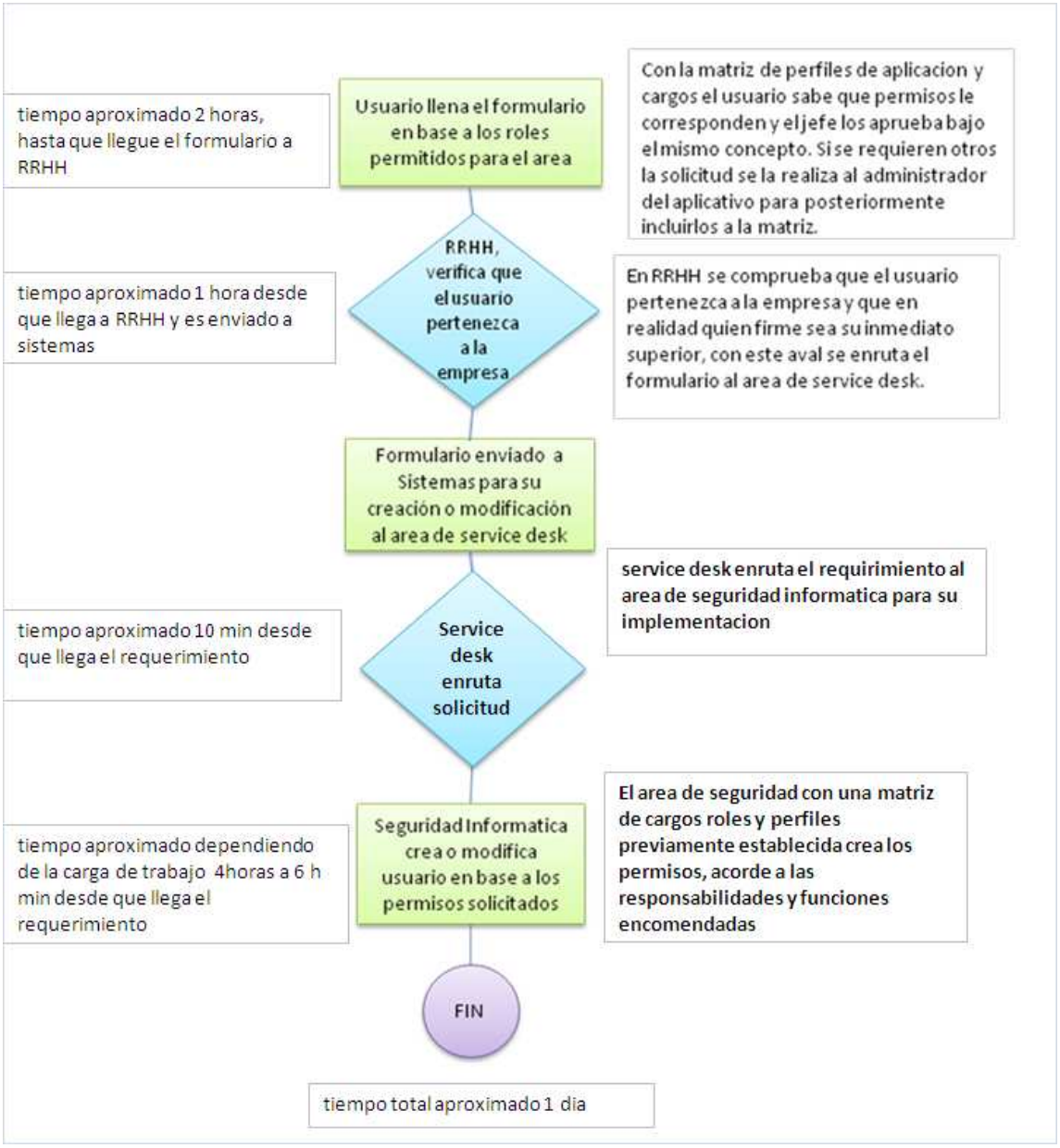



FIG 3.2 Procedimiento propuesto de modificación de cuentas de usuario

En este caso para la eliminación de usuarios, se prevé una alarma se dispare cuando un usuario sea eliminado del sistema de recursos humanos(es decir cuando el usuario ha dejado de pertenecer a la compañía). Esta alarma llega a manera de correo electrónico al área de seguridad quien procederá a buscar sistema por sistema las cuentas existentes de un usuario en particular.

La eliminación en ambos casos (proceso actual y propuesto) es manual.

La automatización del proceso de provisión de cuentas en el que intervienen los usuarios, recursos humanos y departamento de TI puede ser automatizado para mejorar el ambiente de control y mejorar los tiempos de respuesta en la creación, eliminación y modificación de cuentas de usuario. Esto se encuentra detallado más adelante en la sección Soluciones de Seguridad dentro de este mismo capítulo en el apartado “ADMINISTRACIÓN DE IDENTIDADES”

#### 3.2.3.2. Lineamientos para el establecimiento del proceso de manejo de incidentes de seguridad:

**Objetivo:**

Brindar una guía para el establecimiento de procesos de manejo de incidente.

**Alcance:**

Describir una serie de procedimientos a seguir para el establecimiento de un proceso de manejo de incidentes de seguridad informática al interior de la compañía. Esta guía debe ser aplicada por el área de seguridad.

##### *3.2.3.2.1. Definición de incidentes de seguridad*

Un incidente de seguridad informática es cualquier evento adverso que ocurre en un sistema de información causado por la explotación de una (o diversas) falla(s) del mismo, o por la materialización de una vulnerabilidad en componentes de hardware o

software, que impacta en cualquiera de los principios de seguridad de la información. Esta es la definición de incidentes de seguridad sobre la cual se deben establecer los criterios de actuación y seguimiento.

Una vez definido un incidente de seguridad es necesario clasificarlos. Los principios de seguridad informática[57] nos brindan la pauta correcta para tal tarea tomando en cuenta la forma en que estos pueden afectar los mismos parámetros sobre los recursos de TI. Así por ejemplo tenemos la negación de servicio, la inundación de paquetes en la red, el acceso no autorizado, entre otros posibles incidentes de seguridad que pueden darse en la organización. Estos eventos negativos no causan el mismo impacto sobre los principios de seguridad, por ejemplo un ataque de virus puede afectar a la disponibilidad o integridad de los datos, un ataque de ingeniería social a la confidencialidad de la información y un ataque de denegación de servicios una falta en la disponibilidad de los sistemas.

A continuación una lista de los eventos mapeados en una matriz donde se exponen los esquemas en los cuales la disponibilidad, integridad y disponibilidad pueden ser afectadas, en lo posterior si un nuevo incidente es encontrado o reportado se puede realizar cambios sobre la matriz expuesta:

| Eventos detectados | Confidencialidad | Integridad | Disponibilidad |
|---|---|---|---|
| Negación de Servicio | | | X |
| Monitoreo no autorizado de la red, sobre algún elemento que forme parte de un servicio catalogado como crítico. | X | | |
| Acceso no autorizado a datos | X | | |
| Inundación de paquetes | | | X |
| Configuración ineficiente e inadecuada | X | X | X |

[57] Confidencialidad, integridad, y disponibilidad.

| | | | |
|---|---|---|---|
| Revelación de información sensible | x | | |
| Eliminación de archivos o directorios | | x | x |
| Virus | | x | x |
| Modificación no autorizada de datos | | x | |
| Suplantación de datos o direcciones | x | x | X |

Tabla 3.1 Clasificación de los incidentes de seguridad.

Todos estos eventos sobre la base de la clasificación de servicios catalogados como críticos.

#### *3.2.3.2.2. Mitigación del incidente*

Una vez que el incidente ha sido detectado, es decir, cuando la situación anormal este sucediendo (aquella que está fuera de las características definidas como normales para las operaciones de la organización) se debe proceder a adelantar las acciones respectivas para controlar la situación. Se debe realizar un análisis para decidir entre la disponibilidad del servicio y la recolección necesaria de evidencia requerida para analizar los hechos de manera posterior.

La mitigación del incidente incluye los pasos de detección y contención de tal forma que se notifiquen a los interesados y se proceda a recolectar los registros requeridos y evaluar las acciones necesarias para mantener la disponibilidad del servicio afectado, bien sea utilizando un infraestructura alterna o redireccionando las conexiones a sitios confiables o protegidos.

Una vez que se han tomado las acciones necesarias del caso se debe realizar un estudio y análisis de los servicios afectado. En esta etapa es crucial la recolección de datos mediante reuniones con los administradores de aplicativos y aseguramiento de la calidad para establecer los parámetros sobre los cuales estos serán recolectados.

Todos los incidentes de seguridad son catalogados como críticos cuando afecten la disponibilidad de los servicios y/o aplicaciones que constan en la matriz de

aplicaciones críticas. En el caso de que ocurran sobre más de una aplicación los niveles de atención estarán en el mismo orden de cómo fueron clasificados.

#### *3.2.3.2.3. Investigación y análisis*

Luego de restablecer el servicio, en el caso de que fuere necesario, ya sea el hardware o software afectado, se procede a la comprensión de lo ocurrido. Es decir determinar las causas y las consecuencias tratando de responder a las preguntas: qué, quién, dónde, cuando, por qué y cómo. Para ello, basado en un adecuado control de la evidencia y de la escena del incidente se deben aplicar herramientas de cómputo forense para estudiar y conceptuar sobre lo ocurrido.

De manera paralela, se adelantan en un ambiente controlado, los ajustes requeridos para mitigar las vulnerabilidades identificadas, documentando los impactos de las mismas y los correctivos efectuados. Todo el hardware y/o software pasado a un ambiente controlado de pruebas necesita pasar por el proceso de control de cambios, esto es necesario para poder pasar nuevamente al ambiente de producción y restablecer el servicio de una manera adecuada y segura.

#### *3.2.3.2.4. Reporte*

Una vez concluidos los ajustes y se ha concluido la investigación asociada con el incidente, se procede a documentar y generar los informes requeridos tanto para la gerencia como para el área técnica. Este ejercicio debe registrar el conocimiento adquirido luego del evento y plantear un objeto de monitoreo nuevo que puede impactar cualquiera de las otras fases de la atención de incidentes. Toda la documentación generada en los pasos anteriores debe guardarse en una base de conocimientos de resolución de incidentes de seguridad.

Adicionalmente esta fase, exige del equipo de atención de incidentes la generación de métricas de incidentes, basadas en su clasificación y luego analizadas a la luz de los impactos y de los cambios requeridos sobre los componentes de la infraestructura, como una métrica de qué tanto se está comprendiendo y gestionando la seguridad y cómo estos resultados han impactado de manera positiva los

resultados de la gestión de la seguridad informática en la organización. Las estadísticas (indicadores) de atención de incidentes son la carta de navegación de cómo los procesos de negocio se ven impactados y que tan efectivas han sido las medidas de seguridad allí instaladas.

#### 3.2.3.3. Guía para la clasificación de información en procesos críticos.

**Objetivo:**

Brindar una guía para la clasificación de información en procesos críticos.

**Alcance:**

Describir actividades a seguir para clasificar la información en procesos de la compañía con la finalidad de detectar el intercambio de datos sensitivos

##### *3.2.3.3.1. Identificación*

En cada una de las aplicaciones críticas de negocio existe información que debido a su sensibilidad deben ser correctamente identificadas dentro de cada una los procesos que se manejan en la compañía. .

La información es catalogada como sensible cuando sobre ella se ha establecido una característica reservada la cual deberá ser consecuente con los niveles de seguridad que se implementen sobre ella especialmente cuando viaja a través de algún medio.

La información será catalogada como confidencial cuando cumpla los siguientes requisitos:

a.- no se encuentre clasificada como pública de acuerdo a lo establecido en la Ley Orgánica de Transparencia y Acceso a La Información Pública.

b.- Si al ser divulgada podría restarle competitividad a la compañía, como planes estratégicos de negocio que pueden ser aprovechados por terceros para ganar mercado. O bases de datos de clientes corporativos que pueden ser usados por tercero para la apropiación indebida de clientes.

c.- Si al ser divulgada podría provocar pérdida de imagen o daños en sus instalaciones y equipos además de denegación de servicios, como por

ejemplo configuraciones de seguridad en la red de la empresa, mapas de ubicación de centrales telefónicas criticas, ubicaciones de instalación de fibra óptica, etc.

Esta información reservada podrá tener 2 niveles de confidencialidad, medio y alto. El nivel medio es aquel que puede ser accedido por personal interno a la empresa y el alto es aquel a los cuales terceros no pueden acceder por el riesgo que implica su difusión a los intereses de la compañía.

Cada una de las Gerencia elaborará un listado con la información confidencial y el flujo que esta sigue dentro de la compañía, esta información sirve de entrada para el siguiente paso.

#### *3.2.3.3.2. Análisis de Riesgos*

Con los niveles de clasificación determinados se buscan las amenazas que pueden afectar negativamente en cada una de las gerencias de la compañía, en esta fase deben intervenir los gerentes, jefes de área y personal que conozca el flujo de información y el área como tal.

Con las amenazas identificadas, cada uno de los ITEMS de información deben poseer:

- Probabilidad de ocurrencia en función de las vulnerabilidades de cada ítem de información en estudio, elaborado en conjunto con el área de seguridad.

- Identificación de un conjunto de controles o contramedidas[58] que minimizarán la probabilidad de materialización de la amenaza, elaborado en conjunto con el área de seguridad.

[58] Controles.- medidas que se tomaran para evitar riesgos, y contramedidas son las acciones que tomaran para evitar vulnerabilidades. Comúnmente los controles son más abarcativos como las políticas, normas o procedimientos. Las contramedidas son usadas para atacar temas específicos como por ejemplo falta de parches en un servidor o configuraciones necesarias para aumentar la seguridad en un sistema.

***3.2.3.3.3. Entregable:***

El entregable es un documento donde conste la información reservada, con los riesgos más probables (en función de las amenazas y vulnerabilidades) sus controles y el flujo dentro de la compañía. Los controles buscaran minimizar los riesgos existentes de pérdida de confidencialidad integridad y disponibilidad.

### 3.2.4. SOLUCIONES DE SEGURIDAD

Las soluciones de seguridad buscan reducir los riesgos encontrados en la plataforma operativa de la compañía mediante la implementación de lo siguiente:

- Administración y consolidación de logs
- Administración de identidades
- Protección y seguridad en la red
    - Protección de servidores en la red
    - Control de acceso en la red
- Concienciación de seguridad al personal de la compañía

#### 3.2.4.1.Administración y consolidación de logs

***Antecedentes***

La Gerencia Nacional de TI con el afán de tener un mayor control y conocimiento de lo que sucede en toda su infraestructura tecnológica en relación a eventos de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de los sistemas e información, y tomando en cuenta además, las recomendaciones emitidas en las auditorias del capítulo II, relacionados con el tema de recolección y análisis de eventos en los diversos elementos de las que forman parte las tecnologías de información que son administradas por la Gerencia Nacional de TI, ha decido

automatizar el proceso de análisis de logs de eventos de seguridad optimizando así recursos, y los tiempos de respuesta para la mitigación de los riesgos relacionados.

***Situación Actual***

La infraestructura tecnológica de la compañía posee una amplia variedad de elementos de configuración pertenecientes a cada uno de los servicios que presta la Gerencia Nacional de TI, de los que se destacan servidores, bases de datos, elementos de red, elementos de seguridad, y aplicaciones, alguno de estos elementos a su vez brindan soporte a los diversos procesos de negocio.

Todas las tecnologías que conforman los servidores, bases de datos, elementos de interconectividad de red, y aplicaciones, arrojan un amplio número de eventos que son reflejados en archivos de log, poseyendo diferencias estructurales y semánticas que dependen de la tecnología implementada, haciendo que la frecuencia de lectura, interpretación, y correlación entre los distintos eventos sea una tarea de gran envergadura y consuma una cantidad considerable de recursos.

La falta de esta revisión periódica de eventos generados en cada uno de los elementos de configuración de la plataforma tecnológica de la compañía no está garantizando la detección temprana y la recolección posterior de información relacionada con un incidente de seguridad que ponga en riesgo la confidencialidad, integridad y disponibilidad de información y de los elementos de configuración que son parte de los servicios que brinda la Gerencia Nacional de TI en apoyo de los objetivos de negocio.

Los incidentes de seguridad por su parte van arrojando rastros que se distribuyen alrededor de toda la infraestructura tecnológica de la compañía de la siguiente manera:

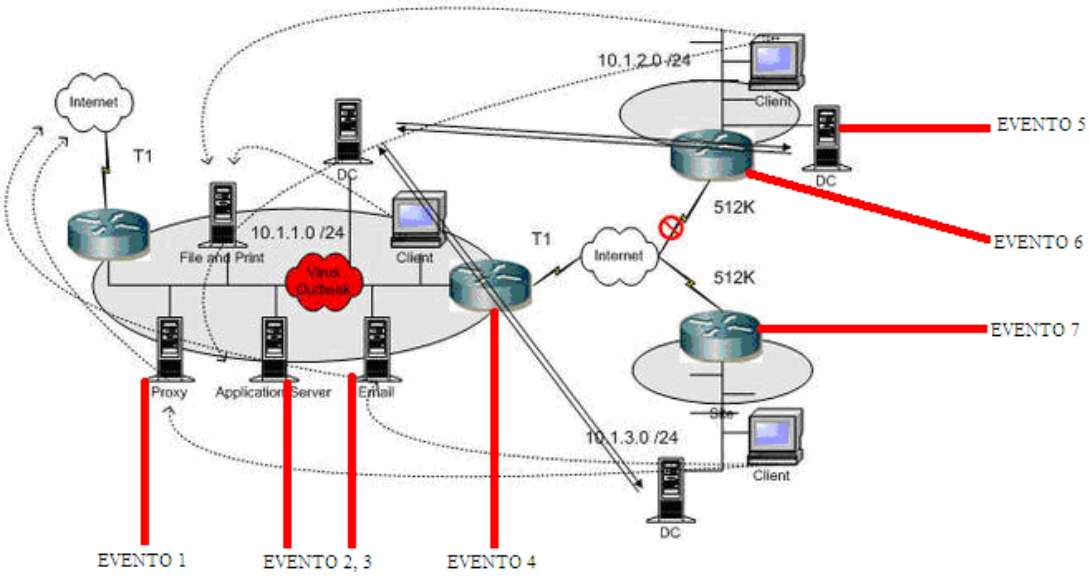



FIG 3.3, Detalle de cómo un evento o una irrupción interna
van dejando huella en todos los elementos de tecnologías de la información

***Alcance***

El alcance es adquirir e implementar hardware y software para la administración de eventos en las tecnologías de información que actualmente administra la Gerencia nacional de TI, en lo relacionado con elementos de:

a.- Aplicaciones
b.- Servidores
c.- Redes
d.- Bases de datos

***Descripción del proyecto***

La plataforma de análisis y consolidación centralizada de eventos, debe estar constituida por:

Hardware y software de propósito específico, diseñado y construido para el propósito de procesar, analizar y consolidar de eventos en las diversas plataformas operativas

de la compañía que son parte de los servicios que brinda la Gerencia Nacional de TI. De esta manera se podrá tener una mejor respuesta en cuanto a la correlación de los diversos eventos generados y una mejor respuesta al análisis en tiempo real.

Los elementos de los cuales LA CNT S.A. conectará al sistema de almacenamiento son:

| BASES DE DATOS | |
|---|---|
| Versión de las bases de datos | Cantidad |
| Oracle 8i Enterprise Edition Release 8.1.7.4.0 | 4 |
| Oracle 8i Enterprise Edition Release 8.1.7.4.1 | 2 |
| Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 | 3 |
| Oracle Database 10g Enterprise Edition Release 10.1.0.4.2 | 3 |
| Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 | 11 |
| Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 | 3 |
| Oracle Database 10g Enterprise Edition Release 10.1.0.4.0 | 2 |
| Sybase IQ 12.7 | 2 |
| Oracle 8i Enterprise Edition Release 8.1.7.4.1 | 1 |

Tabla 3.2, enumeración de las bases de datos administradas por la Gerencia Nacional de TI

| SERVIDORES | |
|---|---|
| Sistema operativo, servidores virtuales | Cantidad |
| Windows 2003 server | 13 |
| RedHat 4 | 7 |
| RedHat 3 | 4 |
| RedHat AS release 3 | 3 |
| RedHat 5,1 | 1 |
| Sistema Operativo, servidores físicos | Cantidad |
| Windows 2003 Server Enterprise edition | 8 |
| Windows 2003 Server | 31 |
| Windows 2000 Server | 14 |
| HP-UX | 2 |
| RedHat Enterprise Linux 4 | 9 |
| SUN Solaris 10 | 4 |
| HP-San Eva | 1 |
| Solaris | 8 |

| | |
|---|---|
| IBM-ESERVER | 7 |

Tabla 3.3, enumeración de los servidores
administrados por la Gerencia Nacional de TI

La plataforma adquirida debe estar en la capacidad de recolectar los eventos en cada uno de los elementos de la infraestructura de Ti detallada en las tablas 3.2 y en la tabla 3.3 además de recolectar los eventos generados por la plataforma CISCO MARS, encargada de recoger logs de toda la plataforma CISCO de la red de la empresa.

***Tipo de solución***

Ser una solución donde sus componentes sean desarrollados con propósito específico en el que se incluya: hardware, sistema operativo, aplicación y base de datos que además deben estar pre-instalados y pre-configurados y licenciados a perpetuidad.

***Compresión***

Asegurar una compresión mínima de 70% para el 100% de los datos de logs recolectados (comparado con el tamaño de los datos de origen), garantizando que de esta manera, se optimice el espacio de almacenamiento de los datos históricos.

***Desempeño***

Poseer componentes tanto el hardware como el software (sistema operativo, aplicación, base de datos) que soporten hasta 2500 EPS (eventos por segundo). Las alertas en tiempo real y las respuestas de correlaciones deben garantizarse independientemente de la tasa de esta tasa de eventos.

***Desempeño bajo altas carga***

Soportar una carga sostenida en recolección y procesamiento mayor al 100% (2500 EPS, eventos por segundo) para asegurar su adecuada operación durante situaciones críticas, p.ej. que se podrían dar en un ataque masivo.

***Agentes***

No necesitar agentes para la recolección de información desde los dispositivos/aplicaciones de origen. La solución debe brindar la capacidad para agregar, eliminar y modificar los dispositivos que son sujetos a la recolección y a la correlación de eventos.

***Filtrado***

No realizar ningún tipo de filtro a los eventos generados en la fuente, estos deberán ser recolectados y almacenados de forma completa, sin que exista ningún tipo de alteración en los datos.

***Normalización***

Realizar ningún tipo de normalización a los eventos generados en la fuente. Estos deberán ser almacenados en su formato nativo sin ningún tipo de cambio.

***Encripción***

Aplicar encripción a los datos que son recolectados y almacenados para su procesamiento. Este proceso deberá ser basado en llaves criptográficas dinámicas que utilicen al menos 128 bits y deberá ser automático sin intervención humana.

***Protocolos de recolección soportados***

Soportar por lo menos los siguientes protocolos para recolección de eventos:

1. Syslog, Syslog NG
2. SNMP
3. Archivos con un formato definido por: coma/espacios/tab delimitadores, otros.
4. ODBC
5. Envío/Recibo de archivos XML a través de HTTP
6. Event Logging API de Windows
7. CheckPoint LEA
8. Cisco IDS POP/RDEP/SDEE

***Reportes***

Ofrecer por lo menos 1.000 reportes pre-configurados entre los que estarán: reportes de seguridad por dispositivo y reportes para regulaciones y buenas prácticas como CoBIT, ITIL y 27002 entre otras.

Permitir el envío de reportes calendarizados en fechas especificas así como también la posibilidad de generar reportes en un tiempo de terminado.

Permitir exportar los reportes a distintos formatos como HTML, XML, PDF, Procesadores de Texto. Brindar la posibilidad de visualizar los reportes vía WEB (https).

***Alertas de seguridad***

Estar en capacidad de generar alertas en tiempo real y debe incluir por lo menos 70 reglas de correlación predefinidas.

Proveer envío de alertas de seguridad cuando alguna política de seguridad configurada en la herramienta sea violada, ya sea sobre la solución en sí ó con los elementos que son correlacionados, por medio del envío de correos electrónicos, mensajes escritos etc.

***Correlación***

Permitir la correlación de eventos basada en estadísticas y en reglas. Además permitir la generación de reglas de correlación complejas para las alertas, según las necesidades de la CNT S.A. Debe soportar sintaxis compleja basada en expresiones estándar y cláusulas de relación tiempo y causa-efecto entre los eventos o circunstancias que se generen en los distintos dispositivos mencionados en las tablas 3.2 y 3.3 y sobre la plataforma CISCO MARS.

Permitir la correlación de eventos por bases de datos, por equipos de interconectividad, y por servidores, brindando la facilidad de interrelacionar eventos por estos segmentos de tecnología.

Permitir la correlación y normalización de eventos mediante la inclusión de datos que permitan determinar ¿Quién lo hizo? ¿Qué hizo? ¿Cuándo lo hizo? ¿Dónde lo hizo? ¿Desde dónde? Y ¿Hacía dónde? ¿Y sobre qué lo hizo? Aplicadas sobre los elementos de bases de datos, servidores, dispositivos de interconectividad, y aplicaciones.

Brindar la opción para calendarizar el marco de tiempo en el cual se realizará la recolección de datos, y debe permitir en un momento determinado el bloqueo o cierre de dicho proceso.

Brindar capacidades de reconstrucción de eventos con datos históricos para investigar sucesos y correlaciones que puedan emerger en un futuro y que no fueron previstas en un inicio por las reglas de recolección.

***Escalabilidad***

Ser escalable permitiendo adaptarse fácilmente al crecimiento futuro, tanto en eventos por segundo como en el crecimiento de elementos de infraestructura tecnológica de la compañía.

***Líneas Base (Baselines)***

Soportar el cálculo y la generación automática de líneas base dinámicas al momento en que los datos son recolectados, logrando traducirlos en “comportamientos normales”, para la obtención de comportamientos anormales, que deberán ser traducidas en alarmas y reportes.

Las líneas base podrán ser utilizadas en consultas, alertas, correlaciones, reportes.

Algunas de las líneas bases deben ser:

- Promedio por minuto

- •Promedio por hora
- •Promedio diario
- •Un minuto especifico de la hora base.
- •Una hora especifica del día base.
- •Un día especifico de la semana base.

***Gestión de Activos y Vulnerabilidades***

Integrar un motor de gestión de vulnerabilidades que permita reducir el número de falsos positivos al analizar y asignar de forma automática valores de importancia relativa a las alertas recibidas de los sistemas IDS/IPS, que posee la CNT S.A.

Permitir determinar la existencia de la vulnerabilidad en los dispositivos antes señalados y permitir entregar una alerta confiable y basada en el nivel de importancia del activo afectado.

***Gestión de Incidentes***

Proveer un sistema de gestión de incidentes de primer nivel, que se integre con sistemas de gestión de tickets externos para escalamientos complejos.

***Análisis Forense***

Proveer un módulo de análisis forense de incidentes, proveyendo una debida cadena de custodia, relacionada con los datos almacenados en la solución.

***Gestión de Ciclo de Vida de la Información***

Soportar y hacer cumplir políticas para la gestión de ciclo de vida de información para lo relacionado con los archivos de logs, de acuerdo con la política de retención definida, es decir que debe poder soportar el almacenamiento de los logs en diferentes tipos de sistemas de almacenamiento para datos es decir: En línea, Cerca de línea y Fuera de línea y con funcionalidades que permitan garantizar la disponibilidad integridad y confidencialidad de dicha información.

***Control de Acceso***

Permitir la integración con Active Directory de Windows para la carga de usuarios y deberá permitir asignar privilegios granulares a cada usuario sobre los módulos que comprende la plataforma emitiendo auditorias sobre los accesos no autorizados.

### 3.2.4.2.Administración de identidades

***Antecedentes***

La Gerencia Nacional de TI, es la encargada de administrar y asegurar las tecnologías de la información (TI) de la compañía, la cual se compone de múltiples sistemas y aplicaciones que diariamente son utilizados por los usuarios internos para el normal desempeño de sus tareas y el correcto funcionamiento del negocio.

Cada uno de los sistemas informáticos requiere de una seguridad de acceso (usuario, contraseña y perfil o rol) para el usuario; el número de aplicaciones a las que tendrá acceso el colaborador dependerá de las funciones que este va a desempeñar.

El usuario que solicita la creación o modificación de la cuenta de acceso y los respectivos permisos para ingresar a determinados sistemas o aplicaciones, puede permanecer un tiempo indeterminado sin desempeñar sus funciones, debido a que el administrador de cada aplicación informática debe ejecutar el proceso de creación o modificación de cuentas y asignación de permisos, conforme su disponibilidad de tiempo.

Una situación crítica se presenta cuando el usuario que ha dejado de prestar sus servicios a la compañía, después de transcurrido algún tiempo, aún mantiene sus cuentas de acceso habilitadas en los sistemas informáticos, esto debido a que el proceso de notificación de salida del personal no ejecuta una transacción en línea.

***Situación Actual***

Actualmente el proceso para la creación de cuentas y asignación de permisos para las aplicaciones informáticas de la CNT S.A. se realiza de forma manual e independiente, es decir que por cada aplicación a la que el usuario requiere el acceso, el administrador de la misma debe ejecutar el respectivo proceso de creación, modificación o eliminación de las cuentas y permisos, lo cual demanda uso adicional de tiempo y recursos que los administradores de las aplicaciones pueden aprovechar en mejorar la productividad con sus tareas cotidianas.

La efectividad de la Política de Seguridad sobre las aplicaciones informáticas, hacen cada vez más necesaria la gestión de identidades de usuarios, por lo que es indispensable contar con un sistema que permita centralizar la aprobación, creación de cuentas y permisos, así como también la modificación y eliminación de usuarios de cada una de las aplicaciones informáticas de la CNT S.A., a fin de minimizar el riesgo de tener cuentas y privilegios no válidos. La automatización de estos procesos permitirá mantener un registro continuo de los cambios en los derechos de acceso y cumplir oportunamente con las auditorias de seguridad y objetivos de la compañía.

De acuerdo a lo indicado anteriormente, es necesario contar con un sistema que centralice la gestión de identidades (cuentas de acceso y permisos) de las aplicaciones informáticas.

***Descripción del Proyecto***

El Sistema de Administración de Identidades sirve para centralizar y automatizar el ciclo de vida y la creación, modificación y eliminación de las identidades de sus usuarios, y garantizar que sólo los usuarios autorizados puedan acceder a los recursos de TI críticos. Esta solución permite reducir los costos de TI, controlar y reducir el riesgo de seguridad global.

Administrar un usuario debería ser un pedido simple, pero puede ser muy difícil de satisfacer cuando se administran identidades de usuarios en entornos de TI

complejos con múltiples aplicaciones, diferentes plataformas y sistemas operativos, y modelos de seguridad incompatibles. Las demandas a las que un administrador de sistemas se enfrenta cuando administra y protege a los usuarios y sus accesos nunca han sido tan grandes.

Previa a la implementación del proyecto de Administración de Identidades y aplicando una metodología aprobada por la CNT S.A., se debe realizar el levantamiento de información, respecto a:

1. Cargos, Roles y Perfiles de los usuarios de todas y cada una de las aplicaciones con las que cuenta la CNT S.A.
2. Definir las aplicaciones asociadas a un cargo, rol y perfil.

Este tipo de solución en su conjunto brinda un único punto de control para todas las identidades de los usuarios y permite automatizar el proceso de creación, modificación, suspensión o eliminación de cuentas y derechos de usuario en todos sus sistemas de la CNT S.A.

La solución debe además:

***Compatibilidad***

Poseer Compatibilidad con AIX, Windows, Solaris, HP-UX, Linux, Oracle, Sql Server, Sybase, DB2.

Integrar la Administración de Identidades de aplicaciones cliente/servidor y aplicaciones Web. Además de la compatibilidad con LDAP de Active Directory, kerberos.

***Gestión de identidades***

Permitir la Provisión/Desprovisión de cuentas, la automatización del flujo de trabajo y el reemplazo automático de contraseñas en modulo de administración de las mismas de forma segura y a través de WEB. El modulo de administración de contraseñas

permiten el establecimiento de contraseñas fuertes para el accesos a los aplicativos de la compañía.

Debe enviar el estado del requerimiento de cambios a los usuarios solicitantes, y permitir que los administradores locales mantengan derechos de crear, eliminar y cambiar cuentas directamente sobre los recursos; estos cambios deben ser detectados y reportados en tiempo real en la solución.

Debe suspender o eliminar cuentas que se detecte no tenga un usuario asociado y suspender o deshacer los cambios hechos a una cuenta reconfigurada automáticamente si se detecta que estos han sido hechos fuera de las políticas establecidas por la institución.

La solución debe ser capaz de detectar y tomar alguna acción, definida con la CNT S.A. cuando se ha creado un usuario en forma local del sistema y no se ha creado a través de la solución de aprovisionamiento.

***Control de acceso***

Permitir definir políticas de control de acceso previamente definidas luego del análisis de roles y perfiles con relación a las aplicaciones.

Ser compatible con cualquier fabricante al momento de integrarse con Enterprise/Legacy Single Sign-On (SSO), y permitir el control de acceso a los recursos de manera centralizada que soporte múltiples métodos de autenticación, principales estándares de la industria y que sean altamente escalables.

***Administración de usuarios y contraseñas.***

Extraer los códigos de empleados definidos en la base de datos de Recursos Humanos de la compañía y configurar y/o construir un identificador único para cada empleado. La forma de nombrar a los usuarios en cada una de las aplicaciones

donde el sistema forme parte deberá ser configurable de acuerdo a las especificaciones y políticas de seguridad de la compañía.

Soportar la asignación dinámica de roles como respuesta a cualquier cambio detectado en los atributos de la identidad. Así mismo debe permitir la posibilidad de una asignación manual de roles y permisos de accesos.

Eliminar usuarios de manera automática al retirar el registro del usuario de una fuente autoritativa. Por ejemplo, al eliminarlo del registro de empleados del sistema de Recursos humanos de la CNT S.A. o al eliminar su cuenta en el Active Directory.

Asegurar la implementación de la Identidad Única. Una vez instalada la herramienta, para cada usuario corporativo debe corresponderle una y solamente una identidad en cada una de las aplicaciones de la compañía. Además debe guardar la información de identidades creadas en un periodo no mayor a 5 años.

Proveer la función de “asignación y suspensión temporal de roles”. Esta función está orientada a evitar brechas de seguridad durante períodos de vacaciones, licencias o reasignación temporal de un usuario.

Generar contraseñas aleatorias y diferentes en el momento en que se asigna al usuario a los sistemas de información, como cuando se solicita el reseteo de la clave de acceso, no deberá existir una contraseña por defecto. Luego de esta actividad el sistema deberá forzar al cambio de contraseña. El sistema también debe proveer la funcionalidad de que el usuario cambie sus contraseñas.

.

Permitir la configuración y uso de diferentes estados (por ejemplo: activo, bloqueado, deshabilitado, etc.) para las personas y/o cuentas de usuario existentes en la organización; el administrador podrá hacer de manera amigable cambios de estado; el sistema debe ser capaz de llevar un log (registro) de estos cambios sin que la persona que originó los mismos tenga opción a modificar el registro.

Validar que la contraseña no sea la misma que el nombre usuario, además de verificar que las contraseñas cumplan con estándares y políticas predefinidas en la CNT S.A., donde se deben establecer periodicidad de reutilización de contraseñas, periodos de valides, numero de caracteres y composición de la misma.

***Cifrado del almacenamiento***

Almacenar la información de usuario y contraseña de manera codificada o cifrada (con algoritmos de cifrado seguro) con el mayor nivel de restricción de acceso posible, de forma que se garantice su confidencialidad e integridad.

***Prestaciones de auditoria***

El software debe permitir al administrador generar reportes de: ¿Quién tiene acceso a Qué?

El software debe generar logs de accesos permitidos, fallidos e intentos de autenticación.

La solución debe proveer un módulo de administración de flujos de aprobación para creación/modificación/eliminación de accesos a los diversos sistemas, con las siguientes características:

1. Debe ser configurable.
2. Debe contar con herramientas para seguimiento de actividades.
3. Debe estar integrada en el mismo portal de autoservicio y auto administración de contraseñas.

***Especificaciones de compatibilidad.***

Ser compatible con los siguientes sistemas operativos en sus versiones mínimas:

1. AIX 4.3
2. Linux versión 4 enterprise

3. Solaris 9
4. Windows Microsoft 2000 server
5. HP-UX v.11.23

Ser compatible con las siguientes bases de datos en sus versiones mínimas**:**

1. Oracle 8i
2. Sybase para Datawarehouse
3. SQL Server 7.0

Ser capaz de crear interfaces para la creación de usuarios en los siguientes aplicativos de la compañía:

***Versatilidad***

Tener la capacidad de integrar plataformas o aplicaciones no soportadas de-facto mediante módulos genéricos o específicos.

Ser capaz de integrarse con 10 módulos y/o aplicaciones de la CNT S.A., entre las desarrolladlas en la compañía y las comerciales, en sus diferentes plataformas para la Administración de Identidades, brindando un Front-End amigable y parametrizable para cada aplicación o sistema.

***Protocolos de Interconexión***

Utilizar entre los puestos de trabajo y/o los sistemas interrelacionados el protocolo de comunicación TCP/IP.

***Reportes.***

Llevar un registro de auditoría seguro y brindar reportes de gestión predefinidos donde al menos se muestre:

1. Lista de todas las cuentas que pertenecen a una persona específica.

2. Lista de todas las cuentas de las personas que pertenecen a un rol determinado.
3. Detalle de las cuentas que existen en un sistema específico.
4. Mostrar todas las políticas (y sus recursos relacionados) que pertenecen a un rol en particular.
5. Listado de las autorizaciones dadas a un individuo en particular.
6. Listado de todas las acciones de aprovisionamiento que cumplen con un criterio en específico, por ejemplo: Listar todas las adiciones o relación de todas las suspensiones temporales de cuenta.
7. Listado de todas las acciones de aprovisionamiento realizadas por determinado administrador.
8. Listado de las solicitudes aprobadas y las rechazadas.
9. Relación de todas las aprobaciones pendientes.
10. Listado de todas las cuentas que han sido suspendidas.
11. Listado de todos los sistemas y aplicaciones que se están aprovisionando.
12. Listado de todas las políticas definidas.
13. Número de cuentas procesadas, de cuentas huérfanas, de cuentas que violan alguna política, cuentas que han sido eliminadas, número de cuentas suspendidas, etc.

La solución debe proporcionar reportes detallados sobre los roles y sus permisos asociados y los usuarios por cada rol.

#### 3.2.4.3. Protección de servidores en la red

***Antecedentes***

El segmento de servidores de la red de La CNT es altamente vulnerable a incidentes de seguridad desde el interior de la compañía, razón por la cual es necesario incluir controles que permitan disminuir la exposición al riesgo que pueden sufrir estos elementos.

Con la adquisición del IPS, se establece controles a la red que nos permiten mejorar la seguridad al impedir que eventos negativos impacten directamente con la productividad de la compañía.

***Alcance***

Adquisición de HARDWARE Y SOFTWARE de propósito especifico para la detección y prevención de intrusiones en la red de servidores de la corporación nacional de telecomunicaciones.

***Descripción del proyecto***

El proyecto de adquisición de un IPS permite aumentar la seguridad interna en un segmento de red donde se situaran lógicamente los servidores que administra la Gerencia Nacional de TI. Este segmento de red será una VLAN diseñada para el efecto, esquematizada según la figura 3.3

Esta configuración permitirá contar con las debidas seguridades de acceso a la red de servidores interna de la organización disminuyendo de manera significativa la exposición al riesgo que pudieran sufrir los activos de información.

Además la solución debe:

***Características de hardware y software (appliance)***

Contar con un puerto de Gigabit en cobre con velocidad de 10/100/1000 y un puerto administración independiente. Ambos puertos de administración deben estar sobre cobre. Estos puertos para su funcionamiento no deben depender de una dirección MAC, ni de una dirección IP, para su funcionamiento.

Ser de propósito específico y tener la capacidad de soportar un throughput de hasta 1000 Mbps.

Filtrar el tráfico de las capa dos a la siete del modelo OSI, y debe ser capaz de

bloquear tipos de tráfico específicos definidos por la CNT S.A. Como por ejemplo el generado por mensajería instantánea, tráfico HTTP a puertos y direcciones específicas, conexiones telnet por mencionar uno pocos.

Tener la capacidad de bloquear tráfico en una sola dirección (hacia la red de servidores o desde la red de servidores) o en ambas direcciones. Y ser capaz de monitorear VLAN´s.

***Prevención y Detección***

Alertar y/o bloquear (según se requiera):

a) Ataques basados en firmas y sobre patrones comportamiento basada en campos específicos del protocolo o aplicación utilizados. Esto implica que el patrón a detectar es buscado dentro de un contexto específico (aplicación, campo, protocolo, etc.), al menos en los siguientes parámetros:

   **Protocolos:** HTTP, SMTP, FTP, RPC, POP3, TELNET, REXEC[59], RLOGIN[60], DNS, IMAP[61], FINGER, DHCP, TFTP, MIME[62], BOOTP, ECHO, DISCARD, SNMP, SNMP trap v1, SYSLOG, SSH, SMB

[59] En host remotos donde este corriendo el demonio rexec, permite ejecutar comandos remotos
[60] Acceso remoto mediante el demonio rlogind en el host destino.
[61] Protocolo de red para acceso a mensajes electrónicos almacenados en un servidor.
[62] Una serie de convenciones o especificaciones dirigidas a que se puedan intercambiar a través de Internet todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos. En sentido general las extensiones de MIME van encaminadas a soportar:

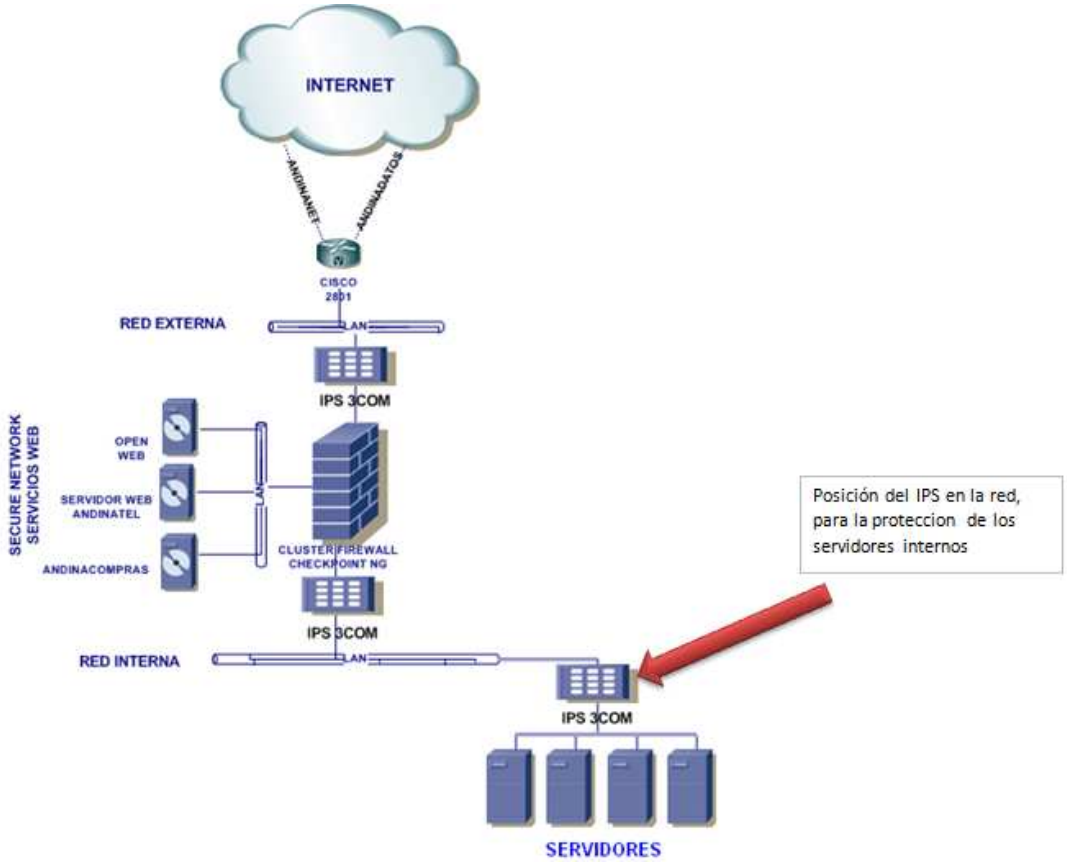



Fig. 3.3 posición dentro de la red de la compañía donde el IPS estará situado.

- (NetBIOS), MS-RPC, VNC, NNTP, IRC, Gnutella, NTP, WHOIS, LDAP, SSL, NBDS, RADIUS.
- **Protocolos de Voz Video Sobre IP:** H.323, H.225, MGCP, SIP
- **Mensajería Instantánea:** AOL-IM, Yahoo-IM, MSN-Messenger
- **Aplicaciones P2P:** BearShare, Gnucleus, Morpheus, Swapper, XoloX, Gnewtellium, Gnutella, Mutella, eMule, eDonkey, ernet, Qtella, LimeWire, Phex, Kazaa, Napster, WinMX.

b) Ataques por análisis de comportamiento, aplicando un análisis heurístico [63]sobre el tráfico para detectar variaciones al tráfico normal que puedan indicar la existencia de un dispositivo infectado con programas del tipo Backdoor, Rootkit, ser parte de una Botnet.

c) Ataques basado en análisis de los flujos del tráfico para identificar los ataques sobre múltiples conexiones. Este método estará diseñado para detectar escaneos y otro tipo de ataques distribuidos (Traffic Anomaly). El método solicitado debe inspeccionar los patrones que indiquen una actividad del tráfico de red anormal como ports scans, escaneo de vulnerabilidades, exploits, además de:

- Tráfico inusual
- Conexiones por segundo
- Umbrales de protocolos (paquetes, bytes, conexiones, etc.)
- Anomalías de host (por ejemplo 200 conexiones de ftp a una impresora en un determinado lapso por ejemplo)
- Análisis de patrones de tráfico
- Análisis de utilización de aplicaciones
- Análisis de utilización de hosts

d) Anomalías en los protocolos que circulan en la red. Es decir una detección y verificación de compatibilidad con RFC para determinar variaciones en los protocolos y aplicaciones.

e) Valores inválidos en la información de las aplicaciones (SQL Injection, scripting shell meta-characters en valores de parámetros para requerimientos desde la web)

[63] Este tipo de análisis se basa en el análisis del código de los ataques y en el análisis de sus puntos críticos, buscando la secuencia o secuencias de instrucciones que diferencian a los virus de los programas “normales”.

Poder ser configurado en diferentes modos: Bridge, Router, transparente y Sniffer (Pasivo). En caso de falla eléctrica o de software el dispositivo debe permitir la opción de by-pass físico del segmento monitoreado de manera que no interrumpa el tráfico. La opción de bypass debe ser configurable manualmente y automáticamente.

Poseer reglas para proteger a la red de ataques de SYN-flood. Se debe detectar y prevenir SYN-Floods asegurando que el hand-shake de TCP se realice correctamente. En el caso que el cliente no envié el paquete de ACK (tal es el caso en un ataque de SYN-FLOOD), luego de un lapso de tiempo configurable, debe tomar la acción correctiva especificada por la CNT S.A.

Estar en la capacidad de proteger la red de servidores contra Gusanos, Troyanos, Spyware, Adware y Keyloggers.

***Actualización de firmas***

Realizar el proceso de actualización de firmas en forma manual o automática. El archivo de actualización podrá descargarse a un servidor local y desde este a la consola de administración. Este servicio de actualización de firmas debe ser diaria y debe contemplar casos de emergencia con tiempo de respuesta tendiente a cero (0).

***Acciones***

Soportar el funcionamiento en modo “simulación”, es decir, que el equipo detecta los ataques pero no toma ninguna acción sobre el tráfico. Además debe poder bloquear tráfico según reglas configuradas a las necesidades de la compañía

Proveer protección inmediata al momento de conectarla a la red con un conjunto de reglas pre-configuradas que prevenga de ataques conocidos.

Proveer protección contra DoS y DDoS (inundación por conexiones por segundo o

por conexiones establecidas), Zombie Recruitment, herramientas de ataque como arpspoof, netcat, entre otros.

Contar con un modulo de software y/o hardware que tome la información de análisis durante un periodo de tiempo y a intervalos regulares y se almacene en un archivo para su posterior análisis ya sea manual o automático con herramientas de análisis de logs.

***Rendimiento***

Tener un rendimiento hasta los 1000 MBPS con una latencia máxima de 1 milisegundo.

Manejar al menos cinco mil sesiones (conexiones bidireccionales) y deberá soportar como mínimo cinco mil conexiones por segundo.

***Tolerancia a fallas***

En el caso de que se instale una segunda unidad, el equipo podrá ser configurado en modalidad de redundancia activa-activa de tal manera que ambos equipos funcionen simultáneamente haciendo balanceo de carga y bloqueando el tráfico mediante el establecimiento de políticas de tráfico homogéneas mediante un sistema de administración centralizado.

#### 3.2.4.4. Control de acceso en la red

***Antecedentes***

La red interna de la compañía debido a varias debilidades detectadas con la implementación de DHCP[64] y la falta de controles de acceso en capa 2 de los puertos físicos de conexión, permiten que un host al ser conectado en un puerto libre adquiera parámetros de configuración que automáticamente le dan acceso a los

[64] Sigla en inglés de Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Servidor.- Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente

elementos de la plataforma operativa como servidores y elementos de interconectividad de red. A esto hay que sumar la falta de controles para la prevención de intrusos en el segmento de la red interna, provocando de esta manera una gran exposición al riesgo en la compañía.

***Alcance***

Adquisición de HARDWARE Y SOFTWARE de propósito especifico para el control de acceso de dispositivos finales [65]a la red de la Corporación Nacional de Telecomunicaciones S.A.

***Descripción del proyecto***

El proyecto permite instalar nuevas funcionalidades en la red de la compañía que permitan tomar decisiones de acceso cuando un host intenta ingresar a sus recursos. Esta funcionalidad se basa en el establecimiento de políticas u otros parámetros de acceso configurables que mínimamente debe cumplir el equipo de usuario antes de poder acceder a la red de la compañía.

Los dispositivos finales que no cumplan con las políticas de acceso deben ser puestos en cuarentena, es decir en una red aislada, hasta que sus parámetros puedan ser remediados hasta ajustarse con las reglas de seguridad de la compañía. Estos parámetros pueden incluir por ejemplo que el equipo ingrese al dominio de la compañía, que tenga un antivirus actualizado, que tenga encendido el firewall de protección de Windows u otro adicional, que estén instalados y actualizados los últimos parches de seguridad, que tengan abiertos solo cierto tipo de puertos, que no tenga software considerado como malicioso, por mencionar algunos casos. De no tener las reglas configuradas la solución brinda la posibilidad de solventarlas por medio de actualización y/o descarga de software o indicaciones que ayuden a la parametrización necesaria para poder brindar el acceso.

[65] Dispositivos finales de usuario son por ejemplo computadores portátiles y de escritorio, teléfonos IP, teléfonos celulares, PDA´s, impresoras.

La solución permite además crear o configurar roles al acceder a la red, que restringen cierto tipo de servicios por ejemplo usuarios temporales que requieren acceso a internet o pasantes con acceso a módulos de software identificados.

El sistema debe permitir autenticar y autorizar, escanear y evaluar, poner en cuarentena e implementar, actualizar y remediar a los dispositivos de usuario final que requieren acceso a la red de la compañía.

Además la solución debe:

***Disponibilidad y capacidad***

Funcionar en un esquema de alta disponibilidad, cada elemento utilizado en la solución debe ser implementado en esquema de alta disponibilidad, con la instalación de dos equipos en modalidad Activo/Pasivo.

Estar en la capacidad de manejar el siguiente volumen de usuarios:

| Sitio | Usuarios |
|---|---|
| Informática | 500 |
| Doral | 500 |
| Droira | 250 |
| Mariscal | 250 |
| Estudio Z | 250 |
| Quito Centro | 250 |
| Ambato | 250 |
| Esmeraldas | 100 |
| Ibarra | 100 |
| Internet | 100 |

Tabla 3.5 dimensionamiento de usuarios por edificio

Soportar varios modos de implementación:

- Implementación de acuerdo a la ubicación física, al borde de la red ó en el núcleo de la misma.

- Implementación de acuerdo al acceso del cliente – capa 2 (el cliente se encuentra en la misma red LAN del sistema o solución), capa 3 (el cliente se encuentra en otros segmentos de red a varios enlaces del sistema o solución).

- Implementación de acuerdo al flujo de tráfico – in-band (sistema ve siempre el tráfico de los usuarios), out-of-band (sistema ve el tráfico del cliente solo durante el proceso de autenticación, posteriores análisis del equipo, y necesidades de remediación).

***Control de Acceso y compatibilidad***

Impedir el acceso a equipos finales de usuario que no cumplan con las políticas establecidas por la compañía con relación al control de admisión en la red:

a Realizar la validación de cumplimiento de las políticas de seguridad por parte de los dispositivos de acceso a la red (Network Access Devices) y con las políticas establecidas

b Validar y asegurar el cumplimiento de políticas de manera simple y transparente para los usuarios, en los casos que una política sea quebrantada, el equipo del usuario generador de la violación deberá ser enviado de manera inmediata y temporalmente a una red segura definida por la compañía

c Ser compatible con los sistemas operativos de Microsoft Windows 2000, MAC y LINUX en sus diferentes versiones.

Bloquear, aislar, y remediar equipos que no cumplen con las políticas de seguridad establecidas por la compañía, previo un análisis de la configuración del equipo. Para el proceso de remediación los usuarios deberán ser redirigidos dentro de un área de red segura previamente definida por la compañía, donde se realizarán actividades de remediación y modificación de parámetros para su posterior acceso. Este análisis se lo debe realizar usando direcciones MAC, direcciones IP.

Ser compatible con sistemas de autenticación como: Kerberos, LDAP, RADIUS, Active Directory.

***Administración***

Permitir al administrador: autenticar, autorizar, evaluar, aislar y remediar usuarios que accedan desde redes LAN Ethernet, inalámbricas, MAN, WAN, VPN`s. Identificando si los dispositivos de usuario cumplen con las políticas de seguridad y modificando parámetros faltantes antes de permitir el acceso a la red.

Permitir realizar el control de acceso a diferentes dispositivos de red, incluyendo: sistemas Windows, MAC, o Linux, equipos portátiles, de escritorio, PDA`s, celulares, impresoras y dispositivos telefónicos IP. Permitir este análisis en al menos: puertos abiertos, infecciones, aplicación de últimos parches, antivirus, antispyware, servicios en ejecución, archivos; previo a permitir el acceso de un dispositivo a la red.

Permitir la creación de múltiples perfiles de usuarios con diferentes niveles de permiso a través de un control de acceso basado en roles con restricciones de acceso a ciertos servicios.

Disponer de revisiones pre-configuradas para al menos:

- Actualizaciones críticas de Windows: Windows XP, Windows 2000.
- Actualizaciones de anti-virus: McAfee.
- IPS checkpoint

Definir el periodo de tiempo después del cual los usuarios debidamente registrados deberán ser nuevamente analizados, basados en una regla definida por el administrador. Además en esta revisión debe permitir obtener una lista del software del equipo.

La solución deberá permitir el monitoreo de todos los usuarios invitados registrados en la red y poder deshabilitar dichas cuentas de manera calendarizada y/o manual.

### 3.2.5. CONCIENCIACIÓN DE SEGURIDAD AL PERSONAL DE LA COMPAÑÍA

La capacitación, la formación y la concienciación de seguridad son elementos fundamentales en la implementación de seguridad en una compañía ya que es ahí justamente donde la seguridad se vuelve más deficiente, por esta razón aunque no existe un objetivo de control de bajo nivel especifico en CoBIT con relación a la concienciación de seguridad es necesario topar este tema e implementarlo

Muchos riesgos inherentes al uso de los sistemas informáticos no pueden tratarse a través de mecanismos de seguridad técnica, por ejemplo la compartición de claves de usuario. Un programa activo de concienciación de seguridad puede reducir en gran medida estos riesgos al tratar el elemento conductual de la seguridad a través de cursos de formación y una aplicación consistente de técnicas encaminadas a generar conciencia.

El programa de concienciación de seguridad debe enfocarse en inquietudes comunes de la seguridad del usuario como la elección de contraseñas, como cuidarlas, el uso apropiado de los recursos informáticos y de tecnologías de la información. Los usuarios son la primera línea para la detección de amenazas que podrían no ser detectables por medios automatizadas. Los usuarios deben aprender a reconocer estos tipos de incidentes y comunicarlos al área pertinente de la compañía para su correcto tratamiento.

El programa de concienciación de seguridad debe consistir en cursos de capacitación en línea, pruebas sencillas para motivar la retención de los conceptos de seguridad, recordatorios como afiches, manuales boletines protectores de pantalla; así como cursos regulares de actualización tecnológica.

Las campañas tienen que estar enfocadas al nivel de la organización que se pretenda llegar; no es lo mismo dar charlas de concienciación de seguridad a personal técnico de la compañía que darlas a los gerentes.

Todos los empleados de la compañía tienen que recibir cuando corresponda capacitación apropiada y actualizaciones periódicas sobre la importancia de las políticas, procedimientos de seguridad. Esto incluye además los requerimientos de la seguridad, las responsabilidades legales y los controles de negocio como por ejemplo utilización del sistema Open, sistema SIGAC, así como también la mejor utilización de los recursos tecnológicos.

Existen varios mecanismos que están disponibles para incrementar la conciencia de seguridad:

- Programas de concienciación y capacitación basados en web
- Recordatorios por correo electrónico
- Políticas y procedimientos de seguridad escritos a manera de folletos y publicados en la intranet.
- Boletines informativos, panfletos, videos y carteles
- Incentivos o premios a empleados que informen acerca de incidentes de seguridad sospechosos
- Revisiones de desempeño

A la par que se imparte la concienciación de seguridad se deben establecer métodos para evaluar que tanto de los esfuerzos de seguridad se está replicando en la conciencia de los empleados de la compañía. Esta retroalimentación sirve para las mejoras continuas dentro del mismo proceso.

Para que el proceso de concienciación de seguridad sea más efectivo tiene que estar dirigido a sistemas, procesos y políticas específicos, y la forma única y específica de

cada organización para hacer negocio, así como a su forma de hacer la seguridad en la compañía.

# CAPITULO 4: ANÁLISIS DE COSTOS

En este capítulo se realizará el análisis de costos de las soluciones de seguridad referidas en el capitulo anterior. Estas soluciones incluyen lo siguiente:

- POLÍTICAS Y CONCIENCIACIÓN DE SEGURIDAD.
- ADMINISTRACIÓN Y CONSOLIDACIÓN DE LOGS
- ADMINISTRACIÓN DE IDENTIDADES
- PROTECCIÓN DE LA RED INTERNA
    A. Control de acceso a la red
    B. Protección de servidores en la red

El flujo de fondos neto que más adelante se desarrollará será un compendio de los proyectos propuestos y estará esquematizado de manera global, sin embargo a continuación se detallará los costos individuales para comprender la naturaleza de cada uno de ellos. Posterior a esto se analizará su viabilidad con un flujo de fondos neto que contempla el valor neto actual; esto se realizara analizando el flujo “con” y “sin” proyecto.

## 4.1 POLÍTICAS Y CONCIENCIACIÓN DE SEGURIDAD

Para la difusión de la política se proponen 3 medios de difusión a través de la intranet, correo electrónico masivo, y a través de la impresión de manuales de bolsillo que contengan la política de seguridad de la empresa una vez que haya sido aprobado por los entes regulatorios.

Un cuarto método de difusión de la política es la concienciación de seguridad (no incluido en los tres anteriores, puesto que en la concienciación no solo se trataría temas concernientes con la política, sino temas diversos como análisis de riesgos, problemas de virus propios de la realidad de la empresa por mencionar algunos ejemplos). La concienciación de seguridad es un programa dirigido a los trabajadores de la compañía con la finalidad de reducir riesgos internos relacionados con la seguridad. Estas campañas han resultado exitosas, según un estudio realizado por

Richard Sparks asesor de Litton Industries demostró que mejorar la concienciación y capacitación de seguridad ha resultado en la mejora más rentable de la seguridad en su conjunto[66]

De los tres métodos antes descritos (difusión intranet, correo electrónico, e impresión de manuales de bolsillo) el único que posee un costo, es la impresión de manuales de bolsillo. Si tomamos en cuenta que el último programa entregado a los trabajadores de la empresa, con relación a seguridad industrial y salud, costó alrededor de 2810 USD con un total 46 páginas, el doble de páginas estimado que contendría el manual de seguridad, podemos decir que el costo estaría bordeando los 1405 USD.

La concienciación de seguridad lo realizaría personal del área de seguridad sobre el área de cobertura de la ex Andinatel. Los gastos relacionados por movilización de un profesional del área son 90 dólares y por el chofer de la empresa 45 dólares con estadía incluida, si las charlas se programan en un grupo no mayor de 20 personas dictados en horarios fuera de oficina se tendría el siguiente cuadro:

| **Cuadro de costos para la concienciación de seguridad** | | | |
|---|---|---|---|
| Concepto | **días** | **viáticos** | **Costo** |
| viáticos fuera de la ciudad | 24 | 90 USD | 2160 USD |
| viáticos chofer fuera de la ciudad | 24 | 45USD | 1080USD |
| **TOTAL DE GASTOS** | | | **3240 USD** |

Tabla 4.1 grupos formados en Pichincha
y provincias para un programa de concienciación

## 4.2. ADMINISTRACIÓN Y CONSOLIDACIÓN DE LOGS [67]

Conforme a los parámetros establecidos en el capítulo 2 tablas 2.1, 2.2, 2.3, los costos ascienden a 146.000 dólares como se muestra en la propuesta de la FIG 4.1

[66] Libro de certificación CISM (Certified Information Security Manager), concienciación de seguridad, CAP V
[67] Logs, término que hace referencia a archivos que son generados por eventos parametrizados en los diferentes sistemas. Estos eventos pueden ser por ejemplo fallas en los discos duros, intentos de acceso, errores al cargar servicios entre otros.

que incluyen además el storage[68] de almacenamiento donde se situarán los logs de eventos de seguridad con ciertas características de compresión y cifrado. Mas detalles sobre la propuesta a continuación:

9. PROPUESTA ECONOMICA

| CUADRO DE PRECIOS ANDINATEL- CONSOLA DE SEGURIDAD ENVISION | | |
|---|---|---|
| **Item** | **Cantidad** | **Valor Total (USD)** |
| **Herramienta de correlación de Logs y Auditoria enVision** | | |
| RSA enVision ES-2560 2500 EPS Appliance (Soporta 2500 eventos/seg) | 1 | $ 78.000,00 |
| SecurCare Extended Maintenance for RSA enVision ES-2560 Appliance for 12 months | 1 | $ 25.000,00 |
| 2.7 TB Direct Attach Storage Array | 1 | $ 36.000,00 |
| SecurCare Maintenance for DAS-200 Storage for 12 monts | 1 | $ 7.000,00 |
| **Subtotal Hardware y Software** | | **$ 146.000,00** |
| **Servicios Asociados a la solución enVisión** | | |
| **Instalación** | | |
| Instalación configuración y puesta en Marcha Envision, incluye Gerencia de Proyectos | 1 | $ 9.690,10 |
| Desarrollo de UDS para 2 aplicaciones especificas definidas por Andinatel | 1 | $ 10.143,26 |
| **Subtotal Instalación** | | **$ 19.833,36** |
| **Capacitación** | | |
| Capacitación Envision Para 8 personas 24 Horas dictada en Quito, incluye 2 Libros originales | 1 | $ 8.038,00 |
| **Subtotal Capacitación** | | **$ 8.038,00** |
| **Soporte y Mantenimiento** | | |
| Servicio de Soporte 7x24 1 Visita de Mtto Preventivo y 3 Correctivas en Sitio, por 1 año | 1 | **$ 13.519,89** |
| **VALOR AGREGADO:** 2 cupos para asistir al a cualquiera de los cursos del portafolio de capacitación de ETEK, los cuales se dictarán en la ciudad de Bogotá | 2 | N/A |
| **Total de la Solución Ofrecida (No Incluye IVA)** | | **$ 187.391,3** |

FIG

Tabla 4.2 Propuesta económica proyecto de consolidación de logs, costos en dólares americanos.

De los costos expuestos en la FIG 4.1 fueron tomados en cuenta para el flujo de fondos de la tabla 4.3 los siguientes:

- Herramienta de correlación de logs y auditoria: En este ítem se incluyen los costos de software y hardware de la solución, incluido el costo de licencias, a esto hay que sumarle los costos de la capacitación al personal encargado de la administración del producto.

[68] Storage, termino anglosajón que refiere a un arreglo de discos duros con la finalidad, en la mayoría de los casos, el de almacenar información.

- Instalación configuración y puesta en marcha: En este valor está incluido el salario de los consultores, costos de implementación, capacitación y parametrización de la herramienta.
- Soporte y mantenimiento: valores de soporte y mantenimiento tanto del hardware como del software por un año.

## 4.3. ADMINISTRACIÓN DE IDENTIDADES

El administrador de identidades consta de dos partes una de segregación de cargos roles y perfiles en cada una de las aplicaciones críticas de la empresa y la parametrización de la herramienta con esta información para adaptarse a las aplicaciones desarrolladas o propias de la compañía. El administrador de identidades es una nueva capa que se crea entre los usuarios y los servicios y actúa como autorizador que permite o deniega acceso a las mismas dependiendo de políticas parametrizables en la herramienta. Cuando una persona se integra a la empresa y su cargo necesita accesos a una aplicación un tiquete de atención o requerimiento se dispara desde recursos humanos hacia la solución de identidades (tal y como el flujo de creación de usuarios). Este tiquete le dice a la solución(administrador de identidades) crear las cuentas necesarias ya sea de red, correo electrónico y acceso a las diferentes aplicaciones. Por lo tanto la solución ya “sabe” de antemano que perfil dentro de la aplicación le corresponde a cierto tipo de cargo; de ahí la importancia de la primera parte de este proyecto. La realización de este trabajo tomará alrededor de cuatro meses con un costo de 30.000 USD con un alcance de 20 aplicaciones, sin embargo en una propuesta recibida este costo está incluido dentro de la implementación del proyecto así como el desarrollo de conectores para cada aplicación, que realizarían la validación de los permisos solicitados y su posterior creación. El detalle de los costos se muestra a continuación:

***INVERSION***

| CANT | DESCRIPCION | PVP TOTAL US$ |
|---|---|---|
| 2000 | CA Identity Manager (Para la gestión de usuarios y Workflow). Se licencia por usuario | $129,400.00 |
| 1 | Implementación y Capacitación de CA Identity Manager | $122,700.00 |
| 1 | Hardware | $5,500.00 |
| | **TOTAL** | **$257,600.00** |

Tabla 4.3 valores de la propuesta económica para el proyecto de administración de identidades, los valores están en dólares americanos.

Aunque los costos de soporte y mantenimiento anual no están incluidos en esta propuesta es conocido que este costo varía entre un 10 y un 15 % del costo de licenciamiento al inicio del proyecto, para este caso el valor estaría bordeando los 13000 y los 19000 dólares, si hacemos un promedio este precio seria de 16000 dólares. Este último precio será tomado en cuenta para el desarrollo del flujo de fondos neto y tomado en cuenta como costo de operación del proyecto.

## 4.4. PROTECCIÓN DE LA RED INTERNA (IPS Y NAC)

Para la protección de la red se recomiendan 2 proyectos un proyecto enfocado a proteger la red del acceso no autorizado de host que no cumplan con parámetros de seguridad impuestos en la empresa y un sistema que proteja a la VLAN de servidores y bases de datos de ataques internos o externos, denominados Control de Acceso a la Red (NAC por sus siglas en ingles) y Sistema de Prevención de Intrusos (IPS Intrusión Prevention System, por sus siglas en ingles) respectivamente.

La tabla de costos aproximados [69]se muestra a continuación:

| COSTOS | IPS | NAC |
|---|---|---|
| Instalación implementación | 10000 | 60000 |
| Hardware licencias | 40000 | 240000 |
| Soporte y mantenimiento anual | 5000 | 20000 |
| TOTAL | 55000 | 320000 |

Tabla 4.4 costo en dólares aproximado de la implementación de proyectos de seguridad de la red

Los costos de implementación incluyen además el costo de capacitación en la herramienta, pago de consultores y técnicos para la implementación de la solución.

Ahora es necesario realizar un análisis de las pérdidas asociado a los incidentes de seguridad y a los problemas por falta de automatización de ciertos procedimientos con es el caso de la administración de identidades.

## 4.5. ANÁLISIS DE PÉRDIDAS RELACIONADOS CON TEMAS DE SEGURIDAD

Como se observan en las tablas 4.1 a la tabla 4.4 en los flujos los costos de inversión a realizar en seguridad parecen tener un costo elevado es necesario realizar un análisis más profundo para encontrar un balance entre la inversión y la seguridad.

Por una parte se tienen los proyectos de políticas de seguridad, difusión protección de la red interna (IPS y NAC), administración y consolidación de logs que van a ser justificados por pèrdidas debido a incidentes ya ocurridos al interior de la compañía y por otro lado el proyecto administrador de identidades que tiene un componente especial, la automatización del proceso de creación de cuentas.

[69] A diferencia de los proyectos antes descritos estos costos son aproximados debido a que las empresas proveedoras de este tipo de soluciones necesitan tener una propuesta formal de inicio de proyecto por parte de la CNT, sin embargo estos precios son muy cercanos a la realidad y fueron otorgados de primera fuente.

### 4.5.1. ANÁLISIS DE COSTOS PARA LOS PROYECTOS DE POLÍTICAS Y CONCIENCIACIÓN DE SEGURIDAD, ADMINISTRACIÓN Y CONSOLIDACIÓN DE LOGS, Y PROTECCIÓN DE LA RED INTERNA (IPS Y NAC).

Es necesario precisar que para el tipo de inversión en seguridad se deben definir nuevos parámetros de evaluación que servirán para poder determinar la viabilidad de un proyecto de seguridad, puesto que no se trata de un proyecto de inversión con el cual una compañía puede tener una renta estimada en un plazo de tiempo.

Para la justificación de los proyectos de seguridad se necesita conocer las pèrdidas aproximadas relacionadas con incidentes de seguridad. A continuación una breve esquematización de las más relevantes en el periodo comprendido entre los años 2003 y 2009.

#### 4.5.1.1. Incidentes de seguridad

A continuación una breve reseña de los eventos de seguridad presentados en la compañía desde el 2003.

- Marzo 2003, problema de Virus en la empresa 2 semanas sin operaciones normales en la compañía.
    - Problemática: una semana sin operación normal del servicio de recaudación.
    - Causas: infección masiva de virus en la red de la empresa causada por usuarios internos de la empresa.
    - Solución, desinfección de virus por personal de la ex Vicepresidencia de Sistemas en toda la compañía, incluye servidores.
- En agosto de 2007 el sistema OPEN tuvo un daño en su base de datos relacionada
    - Problemática: alrededor de 3 días no se pudo ofrecer los servicios de recaudación de manera óptima.

  - Causas: indeterminadas.
  - Solución: Reconstrucción total de la base de datos.
- Finales de 2007, cliente del servicio de banda ancha se comunica con personal de la compañía visiblemente enojada debido a que su información (tipo de servicio de banda ancha adquirido, números de teléfono ,dirección de vivienda) había sido remitida por la CNT a empresa competidora.
  - Problemática: fuga de base de datos de clientes de la compañía.
  - Causas: trabajadores de la empresa implicados en el envió de información.
  - Solución: investigaciones en progreso.
- Marzo 2008, problemas de virus en Riobamba ocasiona bloqueo masivo de cuentas de usuario impide desarrollo de labores en 4 días.
  - Problemática: 4 días de bloqueo continuo de cuentas
  - Causas: infección de virus causada por usuarios internos de la empresa.
  - Solución: Desinfección masiva por personal de la Gerencia de TI en toda la compañía (ex vicepresidencia de sistemas), incluye servidores.
- Agosto 2009, infección de virus masiva, 1 semana sin operación normal al interior de la compañía
  - Problemática: alrededor de 1 día no se pudo ofrecer el servicio de recaudación.
  - Causas: infección de virus causada por usuarios internos de la empresa.
  - Solución: Desinfección masiva por personal de la Gerencia de TI en toda la compañía (ex vicepresidencia de sistemas) , incluye servidores.
- Finales del año 2009 cliente del servicio de banda ancha llama a la compañía informando que gente de ventas de empresa competidora se contacta con esta conociendo de antemano que es cliente de la CNT.
  - Problemática: fuga de clientes de la compañía.
  - Causas: técnicos de la empresa implicados en el envió de información.

- Solución: Separación de relación de dependencia de ese personal con la compañía.

A continuación un análisis de las pérdidas ocasionadas por estos incidentes.

#### 4.5.1.2. Análisis de pérdidas de los incidentes de seguridad

**a.- Pérdidas en el servicio del sistema OPEN**

El servicio del sistema OPEN (motor sistemático de las operaciones de la empresa) tiene un plan de contingencia que se activa cuando no existe disponibilidad del servicio de base de datos o del servidor principal. Cuando este plan se activa tiene un periodo de 2 horas durante las cuales nadie puede acceder, sin embrago luego de transcurrido este tiempo solo el personal de Recaudación[70] puede hacerlo.

Se tiene el siguiente escenario[71], cuando la contingencia se activa:

| Operatividad | Usuarios |
|---|---|
| **Usuarios Open Producción** (sin incluir recaudación) | 1088 |
| **Usuarios Open, Recaudación** | 288 |

Tabla 4.5 clientes solo de la aplicación OPEN, los usuarios Open-recaudación son los únicos que estarían operativos en la contingencia

Es decir que el 26% del personal que tiene acceso al OPEN estaría operativo, cuando se produzca algún tipo de denegación del servicio.

Si realizamos un análisis de costos por pérdidas, por cada hora que OPEN esta sin servicio en recaudación, por alguna falla ya sea de bases de datos o de algún elemento que impida que normal desenvolvimiento de la aplicación continúe, las pérdidas tan sólo operativas serian de:

[70] Personal de la compañía situada en ventanillas que se encarga de realizar la recaudación de la empresa.
[71] Este escenario esta sobre la base de la contingencia actualmente aprobada sobre la cual en caso de fallar el sistema OPEN, se tendría un sistema que alterno con el cual solo las recaudaciones estarían operativas.

Personal de recaudación sueldo promedio 900 dólares esto quiere decir que cada hora la empresa paga por estos servicios 5,63 dólares por hora (900÷160[72]) y al multiplicar por el numero de personal total (antes de que entre a funcionar solo recaudación luego de 2 horas) tendríamos alrededor de 15.493,76 USD (2x5,63x1376) en pérdidas solo en pago de personal. Luego de las dos horas luego de accionada la contingencia las pérdidas por pago de personal (sin incluir recaudación, 1088 empleados) por cada hora seria de 6125,45 (1x1088x5,63). Esto quiere decir que por día las pérdidas son de: 52245,7 USD (15.493,76+(6125,45)x6) al primer día de iniciada la contingencia luego cada da cuesta 49000 USD (6126,45x8).

**b.- Pérdidas software malicioso**

Los virus agudizan las pérdidas de la compañía operacionalmente hablando si tomamos en cuenta que en promedio el 40% del personal de compañía quedo indispuesto de realizar sus funciones al día y si tomamos en cuenta que existen 1800 usuarios conectados a la red de la empresa(es decir usuarios con computador) con el mismo promedio antes mencionado tenemos un total diario de 32.400 dólares (1800x0,4x5,63x8).

Con los rubros antes expuestos se tiene el siguiente esquema:

| PÉRDIDAS TOTALES DE INCIDENTES REGISTRADOS 2003-2008 | | | |
|---|---|---|---|
| EVENTO | PÉRDIDAS POR DIA | DÍAS SIN OPERACIÓN OPTIMA | PÉRDIDAS |
| Fallo servicio OPEN | 52246 | 3 | 156738 |
| problemas de VIRUS | 32400 | 10 | 324000 |
| **TOTAL** | | | **480738** |

Tabla 4.6 pérdidas más representativas relacionadas con seguridad en los últimos 5 años

[72] 40 horas ordinarias de trabajo semanales, según el código de trabajo.

### 4.5.2. ANÁLISIS DE COSTOS PARA EL PROYECTO DE ADMINISTRACIÓN DE IDENTIDADES

Si bien es cierto el flujo de fondos para este proyecto parece un poco elevado es necesario conocer 2 aspectos con relación a la administración de cuentas que se lleva a cabo actualmente en la empresa:

- El acuerdo de nivel de servicio establecido para que una cuenta sea creada, modificada o eliminada tiene un tiempo de 8 horas para su atención y solución.
- El promedio de solicitudes de modificación y creación son entre 15-20 por día.

Si el sueldo promedio (para los usuarios de TI) es de 900 USD, y si tomamos en cuenta que 8 horas es el tiempo de atención de este requerimiento (es decir un día de trabajo) en promedio la compañía pierde por operatividad 45 dólares diarios por cada una de las cuentas que han solicitado ser creadas. Si en promedio el tiempo de atención oscila entre 6 y 7 horas y entre 15 y 20 requerimientos diarios tendríamos alrededor de 507(6x5,63x15) y 789(7x5,63x20) dólares, y al mes un valor que oscila entre los 10140 (507x20) y 15780(789x20) USD, si hacemos un promedio el valor mensual de pérdidas estaría bordeando los 12960 USD. Al año este valor aumenta. Si tomamos como verdad que existen 52 semanas los días laborables serian 253[73] por lo que las pérdidas asociadas a la provisión de cuentas de usuario ascenderían a valores entre los 128271 y los 199617 dólares en pérdidas al año, en promedio 163944 USD.

[73] El código de trabajo expone: *"De las Fiestas Cívicas"Art. 65.- **Días de descanso obligatorio**.- Además de los sábados y domingos, son días de descanso obligatorio los siguientes: 1 de enero, viernes santo, 1 y 24 de mayo, 10 de agosto, 9 de octubre, 2 y 3 de noviembre y 25 de diciembre*",

Las pérdidas totales promedio anuales por concepto de provisión de cuentas de usuario y por concepto de incidentes de seguridad en el periodo 2003 2009 son:

| PÉRDIDAS EN EL PERIODO DE ANÁLISIS 2003-2009 DE ANÁLISIS EN PROMEDIO | | | | | | |
|---|---|---|---|---|---|---|
| **Evento** | **Año 1** | **Año 2** | **Año 3** | **Año 4** | **Año 5** | **TOTALES** |
| Fallo servicio OPEN | 31347.6 | 31347.6 | 31347.6 | 31347.6 | 31347.6 | 156738 |
| Problemas de VIRUS | 64800 | 64800 | 64800 | 64800 | 64800 | 324000 |
| Pérdidas provisión de cuentas de usuario | 163944 | 163944 | 163944 | 163944 | 163944 | 819720 |
| Pérdidas totales promedio anuales | 228744 | 228744 | 228744 | 228744 | 228744 | **1300458** |

Tabla 4.7 pérdidas acumuladas en el periodo comprendido entre 2003 y el 2009

Con los datos de los análisis de los puntos 4.1 al 4.5 podemos realizar un flujo de fondos que nos permita determinar la viabilidad de los proyectos.

## 4.6. FLUJO DE FONDOS NETO TOTAL

Con las tablas 4.1, 4.2 y 4.3 se puede realizar el flujo de fondos neto total tomando en cuenta los proyectos propuesto en el capitulo3.

| DESCRIPCIÓN | Año 0 | Año 1 | Año 2 | Año 3 | Año 4 | Año 5 |
|---|---|---|---|---|---|---|
| (+)Ingresos de Operación | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 |
| (-)Costos de operación | $ 0.0 | $ 57,760.0 | $ 59,492.8 | $ 61,277.6 | $ 63,115.9 | $ 65,009.4 |
| (-) Costos asociados a pérdidas | | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 |
| (-)Depreciación | $ 0.0 | $ 23,100.0 | $ 23,100.0 | $ 23,100.0 | $ 23,100.0 | $ 23,100.0 |
| (-)Amortización | $ 0.0 | $ 82,680.0 | $ 82,680.0 | $ 82,680.0 | $ 82,680.0 | $ 82,680.0 |
| Utilidad antes de participación e impuestos | $ 0.0 | -$ 163,540.0 | -$ 165,272.8 | -$ 167,057.6 | -$ 168,895.9 | -$ 170,789.4 |
| Impuesto a la circulación de capitales (% de los ingresos totales) | $ 0.0 | 0 | 0 | 0 | 0 | 0 |
| Utilidad antes del impuesto a la renta | $ 0.0 | -$ 163,540.0 | -$ 165,272.8 | -$ 167,057.6 | -$ 168,895.9 | -$ 170,789.4 |
| (-)Impuesto a la renta | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 |
| Utilidad Neta | $ 0.0 | -$ 163,540.0 | -$ 165,272.8 | -$ 167,057.6 | -$ 168,895.9 | -$ 170,789.4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Utilidad en venta de activos | | | | | | $ 0.0 |
| (+)Ingresos no gravables | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 |
| (-)Costo de operación no deducibles | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 |
| (-)Valor en libros de los activos vendidos | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 | $ 0.0 |
| (+)Depreciación | $ 0.0 | $ 23,100.0 | $ 23,100.0 | $ 23,100.0 | $ 23,100.0 | $ 23,100.0 |
| (+)Amortización de activos diferidos | $ 0.0 | $ 82,680.0 | $ 82,680.0 | $ 82,680.0 | $ 82,680.0 | $ 82,680.0 |
| (-)Costo de inversión | 530305 | $ 1,405.0 | $ 1,447.2 | $ 1,490.6 | $ 1,535.3 | $ 1,581.3 |
| (-)Capital de trabajo | 210390 | | | | | |
| ***FLUJO DE FONDOS NETO*** | -740,695.0 | -59,165.0 | -60,940.0 | -62,768.1 | -64,651.2 | -66,590.7 |
| Tasa de descuento proyectos de telecomunicaciones | 18.46% | | | | | |
| VAN | ***-933204.39*** | | | | | |

Tabla 4.8 Flujo de fondos neto para todos los proyectos de seguridad propuestos.

Sin embargo es necesario realizar el flujo de fondos neto sin tomar en cuenta los proyectos propuesto para compararlos y elegir el de menor costo.

A continuación el flujo de fondos neto total sin proyecto:

| DESCRIPCIÓN | Año 0 | Año 1 | Año 2 | Año 3 | Año 4 | Año 5 |
|---|---|---|---|---|---|---|
| (+)Ingresos de Operación | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (-)Costos de operación | 228744.0 | 235606.3 | 242674.5 | 249954.7 | 257453.4 | 265177.0 |
| (-)Depreciación | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (-)Amortización | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| Utilidad antes de participación e impuestos | -228744.0 | -235606.3 | -242674.5 | -249954.7 | -257453.4 | -265177.0 |
| Impuesto a la circulación de capitales (% de los ingresos totales) | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| Utilidad antes del impuesto a la renta | -228744.0 | -235606.3 | -242674.5 | -249954.7 | -257453.4 | -265177.0 |
| (-)Impuesto a la renta | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| Utilidad Neta | -228744.0 | -235606.3 | -242674.5 | -249954.7 | -257453.4 | -265177.0 |
| Valor en libros de activos vendidos | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (+)Ingresos no gravables | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (-)Costo de operación no deducibles | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (-)Valor en libros de los activos vendidos | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (+)Depreciación | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (+)Amortización de activos diferidos | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (-)Costo de inversión | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| (-)Capital de trabajo | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| ***FLUJO DE FONDOS NETO*** | -228744.0 | - | - | - | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 235606.3 | 242674.5 | 249954.7 | 257453.4 | 265177.0 |
| Tasa de descuento proyectos de telecomunicaciones | 18.46% | | | | | |
| VAN | ***-995353.1*** | | | | | |

Tabla 4.9 Flujo de fondos neto actual sin tomar en cuenta los proyectos propuestos.

Como se puede observar el VAN (valor actual neto) con proyecto es ligeramente menor que el VAN sin proyecto por lo que se escogería realizar los proyectos si tomamos en cuenta el valor mínimo; además debemos considerar lo siguiente:

a.- Las pérdidas reflejadas en la tabla 4.9 son mínimas, además se debería considerar los costos por:

- ✓ Pérdida de clientes
- ✓ Pérdida de imagen y reputación
- ✓ Pérdida financieras debido a multas regulatorias por fallos en el servicio

Estas pérdidas son más difíciles de cuantificar y necesitan periodos de tiempo prudenciales para poder estimarlos.

b.- La inversión realizada en los proyectos de seguridad no solo minimizan la probabilidad de ocurrencia de lo ya expuesto en el punto 4.6.1. sino otro tipo de riesgos como por ejemplo:

- ✓ Robo de información
- ✓ Denegación de servicios
- ✓ Falta de integridad de datos de transferencia
- ✓ Control de acceso eficiente
- ✓ Manejo de incidentes de seguridad, entre otros.

De presentarse estos eventos (que son probables que ocurran) podrían aumentar los costos de la tabla 4.9 y aumentar la diferencia entre los valores del VAN correspondientes a cada uno de los flujos de fondos y justificar de mejor manera la inversión en proyectos de seguridad.

Estos dos puntos son importantes puesto que determinan que aunque los costos relacionados en la implementación de proyectos de seguridad son ligeramente parecidos (con una diferencia de 62048.71 a favor de los proyectos) esta diferencia podrían aumentar significativamente si no se llegaran a implementar.

# CAPITULO 5: CONCLUSIONES Y RECOMENDACIONES

## 5.1. CONCLUSIONES

- El proyecto de administración de identidades es un proyecto que ayudará a mejorar el ambiente de control dentro de la empresa y reducir costos. Las solicitudes, autorizaciones y asignaciones de cuentas de acceso a aplicaciones se las realiza de manera segura, autorizada y automática. Alrededor de 5000 usuarios se pueden beneficiar de la implementación de este proyecto ya que disminuye de manera drástica el nivel de atención de las solicitudes (aprox. 10 minutos de la herramienta frente a los 360 minutos actuales). La reducción de costos, en este esquema, en un periodo no mayor de 2 años es otra característica importante, ya que el costo del proyecto bordea los 257.000 dólares frente al costo actual que aproximadamente suman 163.000 dólares, esto quiere decir que el valor actual neto (VAN) del proyecto comienza a ser inferior a partir del 2 año (69.000 dólares aproximadamente) con las ventajas ya expuestas.
- Del análisis del flujo de fondos se desprende que en el caso de considerar la implementación de los proyectos frente a mantener el estado actual existe una diferencia en costos de 62.149 dólares a favor de la implementación, pero es necesario mencionar que estamos protegiendo a la organización de:
    - Pérdida de clientes
    - Pérdida de imagen y reputación
    - Pérdida financieras debido a multas regulatorias por fallos en el servicio:
    - Robo de información
    - Denegación de servicios
    - Control de acceso ineficiente

Costos que por su naturaleza son más difíciles de cuantificar, pero que de suceder podrían causar un grave daño a la institución posiblemente superior a al costo total de los proyectos propuestos.

- En el transcurso de este plan de titulación se ha desarrollado la auditoria siguiendo los controles establecidos en el proceso DS5 de CoBIT lo que ha permitido diseñar una estructura de seguridad a medida de la Corporación Nacional de Telecomunicaciones que comprende políticas de seguridad, procedimientos e infraestructura tecnológica de seguridad que en conjunto minimizan las vulnerabilidades encontradas en el transcurso de este trabajo y que se encuentran condensadas al inicio del capítulo 3. Esto es parte del objetivo general planteado en el proyecto de titulación. Los objetivos específicos como:
    - recolección de información por medio de auditorías de seguridad a la infraestructura informática con el método COBIT sobre el proceso DS5 “Garantizar la Seguridad de los Sistemas”; realizado en el capitulo 1,
    - evaluación y determinación del estado actual de la seguridad informática; realizado en el capitulo 2,
    - determinación de vulnerabilidades de la infraestructura informática; realizado en el capitulo 2,
    - diseño de la estructura de seguridad por medio del desarrollo de políticas, procedimientos y soluciones de seguridad informática; ; realizado en el capitulo 3, y
    - un análisis de costos; realizado en el capitulo 4,

  han sido realizados con éxito. Sin embargo es necesario tomar en cuenta que este es un primer paso dentro del mejoramiento del proceso, que dentro de un proceso de mejoramiento continuo donde intervienen las etapas de planear,

hacer, monitorear, se ha llegado a realizar la primera de estas. Un análisis posterior a la implementación de lo propuesto ayudara a ratificar la mejora de la seguridad en la compañía.

- En este trabajo se ha propuesto mejorar el nivel de madurez del proceso de seguridad DS5 de CoBIT “Garantizar la seguridad en los sistemas”. Este nivel fue establecido, previo un análisis, en un nivel 2 y los objetivos apuntalaban a establecerlo en un nivel de madurez 3. Pero la pregunta es ¿porque no mejorarlo a un nivel 4 ò 5?. El nivel de madurez 5 está reservado, por así decirlo, a instituciones donde el manejo de la seguridad es critico y podría afectar a una población en general; como por ejemplo instituciones gubernamentales que manejan información que podría comprometer la seguridad nacional. El nivel 3 de madurez del proceso es un buen inicio para las organizaciones que quieren mejorar su seguridad y proyectarse a un nivel 4 de madurez. Este último es alcanzado cuando la cultura organizacional así lo permite ya implica en gran medida que los empleados cumplan con las funciones de seguridad encomendadas, que se lleve a cabo un análisis de riesgo e impacto de seguridad de manera regular, que los reportes de conocimiento de seguridad sean obligatorios, y que se esté estableciendo la certificación de seguridad del personal; algo que actualmente en la CNT no se tiene y que sería deseable obtenerlo.

- Existen numerosos ejemplos en los cuales se observa como las seguridades implementadas dentro de una red empresarial resultan ineficientes ante una mala configuración o posición de los equipos que la conforman. Por ejemplo lo encontrado sobre el servidor de base de datos Oracle[74], cuyo acceso no pudo ser detectado por el IPS. Aunque existiera un firewall o un IPS entre el usuario y el aplicativo este no podría detener el acceso ya que este no se realizó

[74] Acceso por medio del cual se pueden subir o bajar procesos del servidor del aplicativo

burlando la seguridad implementada o aprovechando una vulnerabilidad encontrada sino por una mala configuración y segregación de funciones dentro del servidor. Estos equipos ven" tráfico válido accediendo hacia un destino valido por lo que no bloquearan dicho acceso. Estas malas configuraciones de equipos permitirían que accesos no autorizados realicen acciones no permitidas que puedan devenir en costos para la empresa. Ni las políticas de seguridad, ni las soluciones de seguridad podrán evitar que situaciones de esta índole se materialicen. ¿Qué hacer entonces? La capacitación y concienciación a los operadores de sistemas, bases de datos y redes en temas relacionados con temas de seguridad sobre las plataformas que operan, así como a los usuarios sobre las acciones permitidas y no permitidas que están dentro de la organización.

## 5.1. RECOMENDACIONES

- Las auditorias sobre los recursos tecnológicos de una empresa necesitan, antes de su desarrollo, una comprensión de los procesos de negocio que en ella se desarrollan. Se recomienda que se entienda la razón de ser de la empresa sus objetivos y sobre todo saber los riesgos que la empresa posee aunque sea de manera subjetiva. No es necesario buscar evidencia de un mal manejo de un proceso (proceso que se audita u objetivo de control) en cada una de las aplicaciones de negocio o procesos para saber que existe una problemática que debe ser subsanada. Si de antemano se conocen los riesgos de TI lo ideal es empezar la auditoria por estas áreas y/o recursos sensibles y ver que está fallando conforme a las buenas prácticas o estándares establecidos así como de las políticas de seguridad aprobadas.

- Un error que se comete muy a menudo es que la tecnología dicta de alguna manera los procesos y procedimientos de una empresa dependiendo de la funcionalidad que esta herramienta presta. Se recomienda que para la

automatización de los procesos o procedimientos de negocio se tiene que establecer la forma en que las herramientas deben funcionar, es mucho más fácil automatizar algo que continuamente se hace, que implementar un procedimiento dictado por una herramienta; no olvidemos que detrás de los procesos de negocio existen personas y estas son más difíciles de adaptarse a los cambios.

- La seguridad de los sistemas de información tiene que implementarse acorde a la criticidad que representen estos activos para la empresa. Esta criticidad no la dan el personal dentro del entorno de TI, sino las necesidades del negocio, es decir la alta gerencia y sus objetivos. Entiéndase que la alta gerencia no va a indicar que cierto servidor es crítico, sino que TI le dice al negocio que debido a tal objetivo estratégico ese servidor es crítico. Cuando estas necesidades u objetivos cambien es muy probable ciertos activos de información dejen de ser críticos y con esto que los objetivos de seguridad también lo hagan. Por lo tanto los se recomienda que los primeros pasos que hay que dar para implementar un esquema de seguridad en empresas donde no exista un proceso de seguridad maduro es:

  **Documentación de los elementos de TI:**

  a.- La documentación a manera de inventario es fundamental para poder entender las limitaciones tecnológicas que una empresa posee y es la base para la clasificación de activos de información. Este inventario tiene que ser lo más detallado posible por ejemplo en caso de servidores:

  Procesadores instalados, capacidad de procesamiento, marca del procesador, tipo de discos de almacenamiento, tipo de arreglo de discos, capacidad de memoria, memoria instalada, sistema operativo, versión del sistema operativo

  Para el caso de elementos de red: se puede partir de la capa física determinando el tipo de enlaces existentes fibra o Ethernet, tipo de

switches conexiones con los routers donde se incluya información de los puertos físicos inclusive, mapas de red , tipos de firewall e IPS entre otros.

Toda esta información permite conocer los recursos de TI y la forma como los objetivos de TI pueden acoplarse a los objetivos de negocio.

**b.- Clasificación de servicios o procesos críticos**

Mediante esta clasificación de procesos y/o servicios la empresa puede enfocar los esfuerzos de seguridad sobre los elementos que conforman ese servicio. Un servicio se compone de un gran número de componentes como servidores, bases de datos, aplicaciones, acceso a usuarios, redes entre otros si falla uno de estos componentes el servicio queda fuera con las implicaciones que tenga esto para el caso. Por lo que se debe en el momento que se determinan los elementos críticos de TI con relación a objetivos (procesos/servicios) realizar un plan de auditoria de estos elementos con la granularidad que se detecte sea la necesaria para el negocio.

**c.- Identificación de amenazas y vulnerabilidades**

En esta etapa se identifican las amenazas que pueden sufrir los activos de información en la empresa, esta identificación está en función de una probabilidad. Esta probabilidad a su vez está en función de las vulnerabilidades del sistema que se esté estudiando, es decir que si existe una amenaza para una deficiencia dada en el sistema y el sistema en estudio esta parchado contra esa debilidad o por alguna medida de control, la probabilidad de ocurrencia es mínima. Esta etapa sirve de entrada a otro gran proceso dentro del entorno de TI que es el Plan de continuidad del negocio. Se podría decir que luego de esta etapa lo que sigue es la identificación de las medidas o actividades que se desarrollan luego de que los controles no cumplieron su objetivo y el incidente se materializó.

Con los anteriores ítems determinados se pueden empezar a imponer controles de seguridad, en base a una política de seguridad previamente

establecida y en base a objetivos de área y de negocio. Las métricas son importantes para verificar que tan bien están minimizando los riesgos. Esto puede venir de diferentes fuentes como por ejemplo análisis de vulnerabilidades, control de parches etc.

- Se recomienda mapear los incidentes y su impacto en la confidencialidad, integridad y disponibilidad, ya que no solamente facilitan la comprensión y alcances que pueden tener los mismos sobre el negocio, sino que se orienta las medidas preventivas y correctivas requeridas para fortalecer la gestión de seguridad de la información. Complementario a lo anterior, se requiere una estrategia de tratamiento de los incidentes de seguridad que permita actuar con oportunidad y efectividad para limitar los impactos que el mismo pueda tener sobre los procesos de negocio. Dicha estrategia de tratamiento debe ser operacionalmente viable y práctica para enfrentar las amenazas que advierte la presencia del incidente.

- Los proyectos de seguridad tienen que justificarse y la forma más acertada de hacerlos es a través de los costos asociados a pérdidas y las probabilidades de ocurrencia; esto puede estar o no con relación a incidentes ya acontecidos. Por lo tanto se recomienda hacer visible esta perspectiva a la alta gerencia para que observe los costos que puede incurrir la organización en caso de materializarse un evento negativo así como también las medidas que deben seguirse para restablecer los servicios al estado normal de operaciones. Sin embargo es necesario completar esta información con las probabilidades de ocurrencia aun cuando el evento no se haya materializado en la empresa, por ejemplo ataques de páginas web recurrentes a empresas del mismo sector comercial. Aún cuando no hayamos sido víctimas de este tipo de ataques si conocemos de antemano que las páginas web del país por ejemplo están siendo atacadas es muy probable que la nuestra sea víctima de este hecho,

por lo cual las acciones contingentes para este hecho se deben prepara no sin antes hacer establecido los debidos controles preventivos y detectivos para evitar la materialización del incidente.

- La seguridad no es asunto de un área sino un problema que se lo abarca atravesando toda la organización desde las instancias más altas, desde la alta Gerencia, hasta el personal de limpieza. Se recomienda que todo el personal de la organización tiene que estar comprometido en los temas de seguridad, no olvidemos que existen tres pilares fundamentales donde se apoya la seguridad que son los procesos, la tecnología y el personal. El más débil de todos estos son los recursos humanos y de estos depende en gran medida los niveles de seguridad de una empresa. La importancia de las políticas de seguridad y de los planes de concienciación de seguridad enfocados en disminuir los riesgos de seguridad ligados con el personal son tan importantes como las soluciones de seguridad que se implementen.
- La concienciación de seguridad es uno de los elementos claves para mejorar la seguridad en una empresa ya que depende en gran medida del cumplimiento individual. El estudio de Richards Sparks (consultor de litton industries) menciona que RCERT había adquirido a costos considerables tecnología para mejorar la seguridad sin embargo el riesgo continuaba siendo el factor humano. Los niveles de riesgo disminuyeron solo cuando se puso en marcha un programa de concienciación y capacitación que incluyo a 90.000 usuarios y 2000 empelados de TI. Se recomienda por lo tanto capacitar al personal que recién está ingresando a la empresa o el que ya pertenece a ella para dotarlos del conocimiento y habilidades necesarias para satisfacer los requerimientos de seguridad específicos es primordial para el mejoramiento del ambiente de seguridad en una empresa u organización.
- Nada está totalmente dicho en el tema de seguridad lo que se ha plasmado en este plan de titulación es sólo un punto de vista del cual muchos de ustedes diferirán. Lo importante de este trabajo sin embargo es mostrar como las

actividades de TI se relacionan estrechamente con los objetivos de negocio y como estas actividades deben asegurarse para que las metas primarias no sufran desfases que puedan ocasionar que la empresa tenga pérdidas de algún tipo, por ejemplo lo sucedido con la aplicación Andinacompras un esfuerzo de TI que fue considerada critica debido al objetivo de transparentar las compras de la compañía a través de un portal WEB, luego de ese periodo de tiempo fue dado de baja por el portal “Compras Públicas” debido a un giro dado por ordenes gubernamentales. Por lo que fue excluido del análisis de este plan de titulación.