LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA CEDULA MILITAR INTELIGENTE DE LAS F.F.M.M.

FERNANDO ANDRES MURILLO POLANIA
CÓDIGO: 2600771

ANTEPROYECTO DE GRADO PRESENTADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN ADMINISTRACIÓN DE LA SEGURIDAD.

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD
ANTEPROYECTO DE GRADO
BOGOTÁ 2013.

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA CEDULA MILITAR INTELIGENTE DE LAS F.F.M.M.

Resumen

Los Controles de Acceso en cualquier institución, al ser parte de los primeros anillos de protección que se encuentran en el esquema de seguridad corporativo, deben caracterizarse; en su funcionamiento y alcance; por ser verdaderas herramientas que permitan validar, inferir, controlar y dinamizar el proceso de entrada & salida del personal que visita temporalmente las instalaciones. De allí, que la especialización y funcionamiento de controles de acceso de alta performance, requieren un extenso análisis, especificación, desarrollo a la medida; que permita integrar diferentes dispositivos de ámbito electrónico, físico e informático, validando y transaccionando en tiempo real , de manera eficiente todos los datos resguardados en servidores de alta disponibilidad, integridad y confidencialidad; de cada visitante que genere un evento de ingreso o salida, todo a través de un documento único e inteligente sin importar el tipo de guarnición ni el tipo de servicio que dicho visitante solicite.

Palabras Clave**:** seguridad, acceso, control, conectividad, transacción, gestión documental, gestión de riesgos.

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA CEDULA MILITAR INTELIGENTE DE LAS F.F.M.M.

Introducción

Cuando los controles de entrada & salida son vulnerados fácilmente; cuando las políticas inmersas en ellos son insuficientes; situación que muestra ineficiencia en la operación e in-concordancia con las necesidades de protección de las entidades oficiales del estado; cuando por la ausencia de controles de acceso adecuados, se generan brechas ante la coyuntura actual de inseguridad que enfrenta el país; es imperativo contar con elementos activos de seguridad física que, detecten, retarden y que permitan una respuesta oportuna por parte del dispositivo de reacción allí dispuesto. Estas medidas además deben generar disuasión de la actividad delincuencial y terrorista del enemigo, quienes en la situación actual, encuentran un sin número de oportunidades para materializar sus objetivos de alto valor estratégico en el conflicto armado que vive el país.

El anterior análisis toma mayor relevancia en aquellas entidades oficiales que están adscritas al ministerio de defensa nacional, como lo son batallones, brigadas, unidades militares, clubes, Universidades, Hospitales y dispensarios entre otros; ya que enfrentan valoraciones de Riesgos muy altos ante amenazas frecuentes por la misma situación que afronta el país; la probabilidad de materialización de incidentes de Seguridad son altas, y las consecuencias se pueden clasificar como fatales; análisis que denota que es imperativo que estos Riesgos sean atendendidos de manera inmediata por parte de la dirección general.

Teniendo presente que; en la mayoría de los esquemas de seguridad de las unidades anteriormente descritas no se cuenta con la implementación de herramientas versátiles de control de acceso en su infraestructura física, se abre la posibilidad de ejecución de diversos ataques, accesos no autorizados, infiltración, penetración, hurtos, sabotajes; entre otros incidentes; que pueden poner en riesgo la vida, honra, bienes, imagen, activos tangibles e intangibles de las unidades del sector defensa de la Nación.

La ausencia de sistemas automatizado de control, que otorguen de manera eficiente y veraz, la información necesaria para autorizar o denegar el acceso a las unidades militares en las que diferente tipo de personal requiere servicios, permite proponer una oportunidad invaluable de mejora en los esquemas de seguridad nacional; y a su vez, la entrada en uso de un documento inteligente; que suprima los demás documentos de uso oficial; y que contenga la llave a la información integral de cada miembro de la fuerza, acción que permitirá ampliar el rango de aplicación a diferentes controles y medidas de seguridad, así como a la generación de informes Ejecutivos para manejo administrativo y de recurso humano.

Una solución con enfoque holístico de la Seguridad

La definición en un entorno seguro implica la necesidad de estudiar varios aspectos y de establecer una infraestructura que dé soporte a los servicios de seguridad que se quieren proporcionar. Muchas de las organizaciones actualmente cuentan con infraestructura basada en sistemas electrónicos y de control físicos que requieren atención masiva e ingreso simultaneo de

diferente tipo de personal; las F.F.M.M de Colombia no son la excepción. En las instalaciones de las diversas unidades militares; se requiere día a día; que en el ingreso de personal se debe inferir las acciones específicas a desarrollar, por ello es necesario establecer políticas de seguridad y control para impedir, detectar y corregir amenazas que hagan vulnerables sus instalaciones, los activos allí se encuentran así como el personal que allí labora.

Por Todo lo anterior este proyecto se basa en la premisa de dar los lineamientos para generar un documento único inteligente que integre la mayoría de la documentación oficial que sirve como identificación y posterior acceso a las unidades militares para así mejorar la situación actual de seguridad física que presentan los esquemas de cada una de las unidades militares de las F.F.M.M, por las falencias que se presentan al no tener centralizada la información que permita el direccionamiento del acceso o denegación del mismo, de su personal activo, retirado administrativo y visitante

Figura 1. Propuesta Grafica del Documento Cedula Militar Inteligente.

Fuente del Autor.

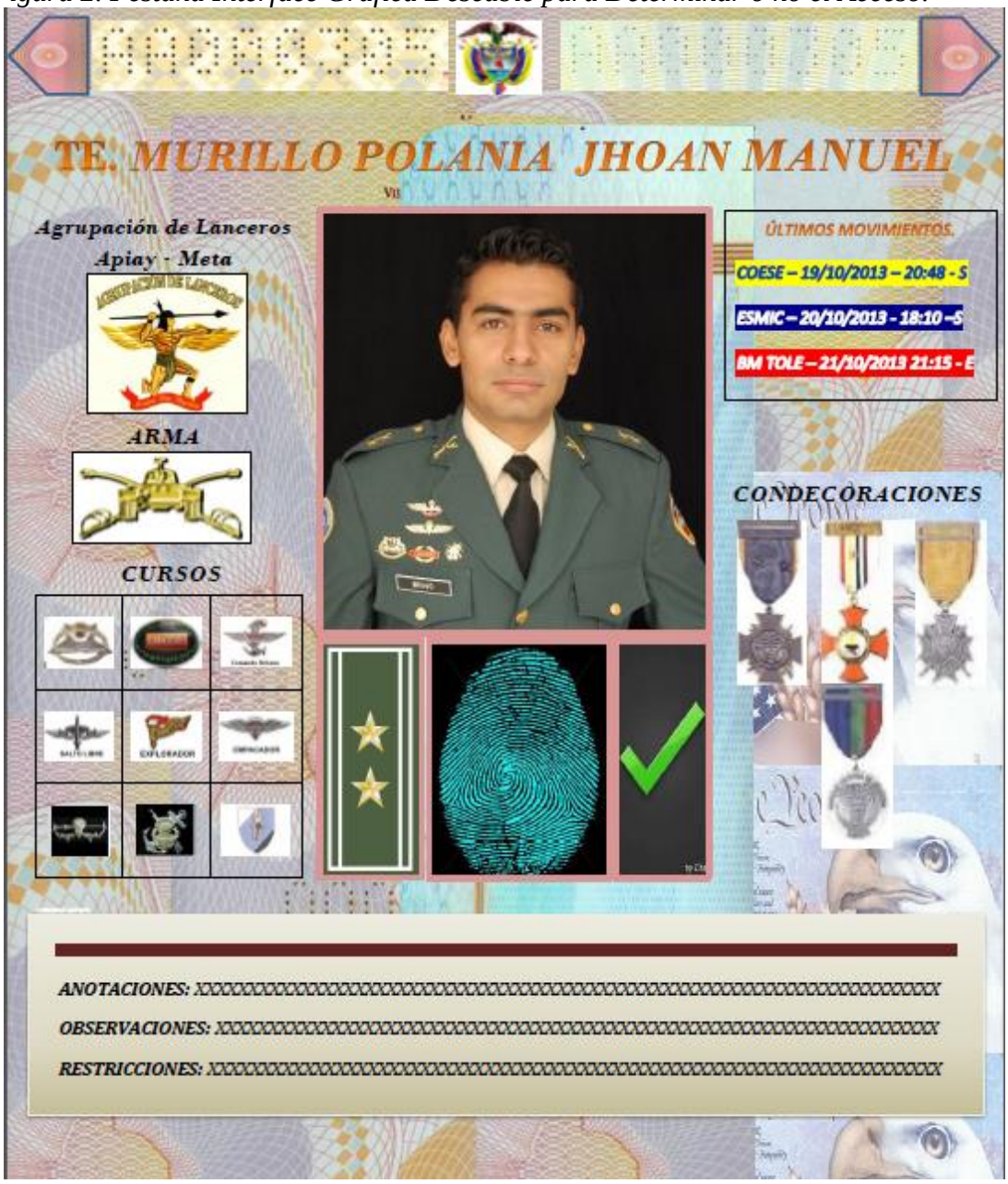
Así pues, el desarrollo de este trabajo quiere dar respuesta a escenarios nefastos que cada vez son más comunes en nuestro país, que han sido analizados y utilizados por el enemigo, generando golpes certeros a la Fuerza pública y de paso a la institucionalidad.

En el éxito de una intrusión, una vez franqueadas las defensas perimetrales, se sucede el compromiso de múltiples activos; que a veces son irremplazables. Existe un flujo de accesos permanentes, personal infiltrado y mal intencionado que dibujan un camino completamente contrario a lo que debería ser aceptable; procedentes desde el exterior de las instituciones y contrarios a las leyes, que crean un puente de entrada a los linderos internos trazando una tendencia cada vez más anómala y peligrosa. El personal de Seguridad y el Gobierno organizacional, víctimas en este caso, que en ese momento, se encuentran administrando seguridad de manera displicente en las sedes infiltradas, nunca notan nada extraño en el momento; ya que solo es posible determinar la magnitud del error cuando el incidente se materializa y estalla la bomba de tiempo que culmina en la tragedia.

Por la anterior Reflexión, se evidencia la necesidad de implementar soluciones efectivas, basadas en herramientas tecnológicas encaminadas y soportadas en los lineamientos plasmados en este proyecto, buscando encontrar las mejores prestaciones al usar nuevos productos, y ahondando en la investigación a fondo de los requerimientos técnicos de Conectividad, Diseños y administración de la Información que conlleve a la puesta en marcha de la solución integral garantizando la seguridad en el acceso sincronizados con protocolos generalizados de cada guarnición y los que oficialmente tenga estipulados o estipule la Institución, corrigiendo la

operatividad como lo exigen las condiciones de seguridad actuales, dejando así a un lado, el manejo de la Seguridad que se genera según la percepción y recursos de la unidad, y de las disposiciones de su administrador de turno con el uso de herramientas y controles de acceso convencionales que limitan el control a lo conocido in situ dejando espacio a la confianza, subordinación y exceso de buena fe del operador o militar de turno.

Figura 2. Pestaña Interface Gráfica Deseable para Determinar o no el Acceso.


TE. MURILLO POLANIA JHOAN MANUEL
Agrupación de Lanceros
Apiay - Meta
ARMA
CURSOS
ÚLTIMOS MOVIMIENTOS.
COESE – 19/10/2013 – 20:48 - S
ESMIC – 20/10/2013 - 18:10 –S
BM TOLE – 21/10/2013 21:15 - E
CONDECORACIONES
ANOTACIONES: XXXX

Algunas de las tareas técnicas más relevantes que se llevaran a cabo a lo largo del desarrollo del proyecto serán el manejo de Documentos Inteligentes (Tarjetas tipo chip 128 bits), Solución de conectividad general, Tramas XML(Datos Quemados), MPLS Transaccional, Software robusto (C#Char .NET), Metodología RUP y UML, Análisis y diseño, Pruebas de stress y de carga, Formulario Tipo pasaporte (Interface gráfica),Elementos de captura, Base de datos centralizada, Redundancia, Capacitación y protocolos de acceso, Dispositivos de lectura procesamiento y trasporte de datos, Seguridad Informática (integridad, confidencialidad y disponibilidad), Transacciones, Gestión de información, Logs del sistema, Data Center, Contact Center, Protocolo de procesos, Casos de éxito, Simulación (picos y colas), Detección de Intrusos efectiva, Pruebas de vulnerabilidad y penetración y Gobierno de la Información.

Unificación Documental, nueva era digital de gestión de información

En la actualidad, a cada individuo de la sociedad que genera una relación comercial, laboral o de ámbito social con cualquier entidad sea de carácter privada o pública; en dicha relación; generalmente la manera para identificarla o catalogarla es la entrega de algún código, documento, contrato o carnet que debe presentar en repetidas ocasiones para que la interacción entre los procesos definidos tenga un inicio y de allí se desprenda el servicio. Es justo ahora, cuando al analizar la facilidad de suplantación, falsificación e inseguridad que genera un simple documento; que no arroja más información que la que pueda percibir el individuo que la solicita; aún más cuando una institución genera diferentes servicios a sus conglomerados, y para cada uno de esos servicio se requiera un documento adicional, inevitablemente encontramos la dispersión de procesos y la redundancia de operaciones innecesarias al no contar con un procedimiento de

unificación documental; que generaría mayores prestaciones así como servicios, y a su vez practicidad y seguridad en los lineamientos institucionales.

La unificación documental en la fuerza pública, permitiría abolir el uso de diferentes documentos como lo son Cedula Militar, carnet de servicios médicos, Carnet del club militar, carnet de guarnición a la que ese agregado, carnet de la escuela según el arma a la que pertenezca, hoja de vida militar entre otros, todos ellos inmersos en un único documento tipo tarjeta con circuito integrado (TCI) de 256 bytes de uso [1] (LPS Software & soluciones TI, 2008) criptográfico que ampliara las posibilidades de identificación y autenticación, ya que se pueden almacenar de forma segura certificados digitales o características biométricas en ficheros protegidos en la Central Documental, y la llave de la transacción estará dentro de la tarjeta, de modo que estos elementos privados se mantengan seguros, así como las operaciones de autenticación se realicen a través del propio chip criptográfico de la tarjeta.

Conectividad, Diseño y Desarrollo base operacional de la Solución

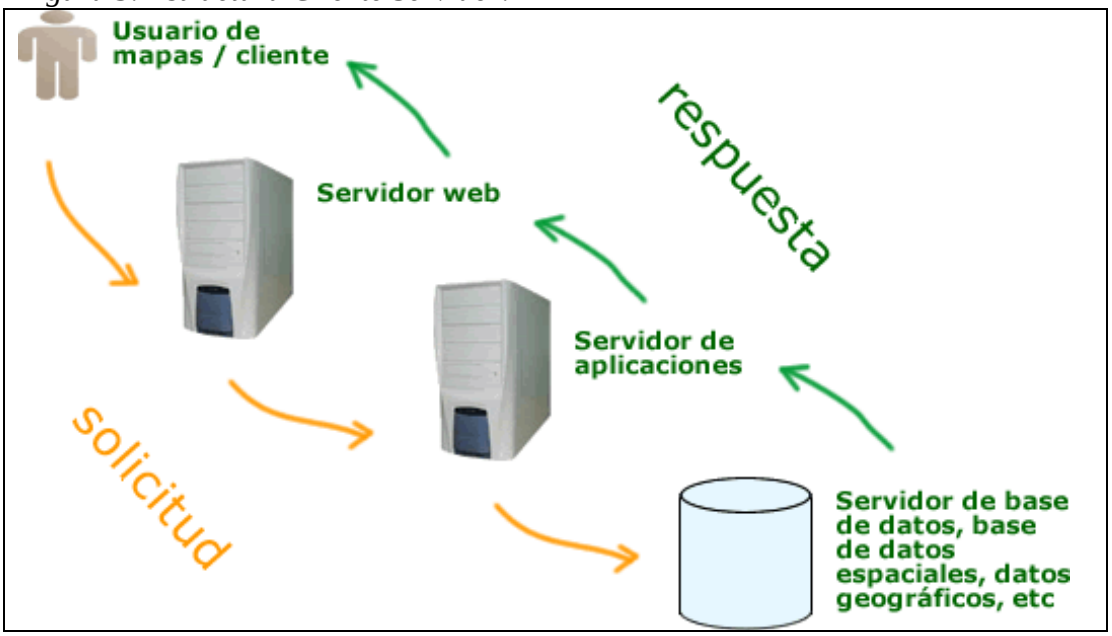
Ya habiendo definido la llave que nos da acceso a la operación de consulta; teniendo claro que deben existir parámetros de entrada, proceso y Salida los cuales deben generar interacción y respuestas; es necesario definir los lineamientos de conectividad, Diseño y Desarrollo que convergerán simultáneamente en el multiproceso operativo, que deben contener los diferentes servicios de conectividad para la plataforma cliente servidor, el diseño de la solución web, ahondando desde la concepción de las estructuras de los datos almacenados y las sentencias de consultas y transacciones que debe soportar y su interface gráfica, así como el desarrollo de

solución en código computacional de alto nivel en las Metodologías de Desarrollo apropiadas, contemplando desarrollo con arquitectura de software y minería de datos que permita llevar a cabo una solución robusta flexible y eficiente.

Esquemas de Conectividad y cobertura de servicios

Este punto de la puesta en marcha del proyecto "cedula inteligente para las F.F.M.M", toma alta relevancia, como se van a disponer los canales de conexión y cómo será la arquitectura de conectividad apropiada que permitirá la estructuración de las autopistas de datos de la solución que en su concepción normal se plantea desde un esquema Cliente Servidor, y debe establecerse como una Red Privada.

Figura 3. Estructura Cliente Servidor.

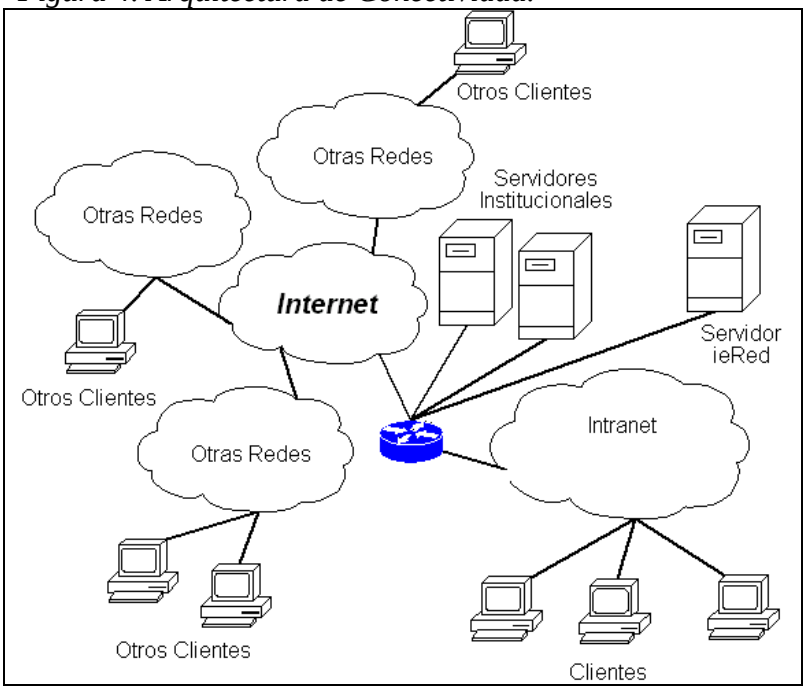


Fuente. www.mapasymapas.com.ar

Proponer la arquitectura de Conectividad para la red de trabajo que se quiere establecer en el proyecto, requiere la abstracción de los componentes de la arquitectura como tal: muchas veces sujeta a la disponibilidad e infraestructura que puedan brindar los proveedores de ISP o los Carriers de Telecomunicaciones que puedan establecer los canales de Comunicación necesarios para la solución. Otro parámetro importante se basa en conocer la dimensión de uso del recurso, nivel transaccional requerido, ya que de esta manera se pueden dimensionar los tipos de Canales, señalización y velocidades apropiadas que serán puntos claves para los tiempos de respuesta que exige la Solución.

Otros puntos que se deben contemplar, ya que pueden modifican la arquitectura del esquema general de conectividad, son la Redundancia, Nivel de Servicio, Operatividad Off-line, puntos de actualización, Backups de la Información, Pruebas de Carga, Pruebas de stress, balanceadores entre otros.

Figura 4. Arquitectura de Conectividad.



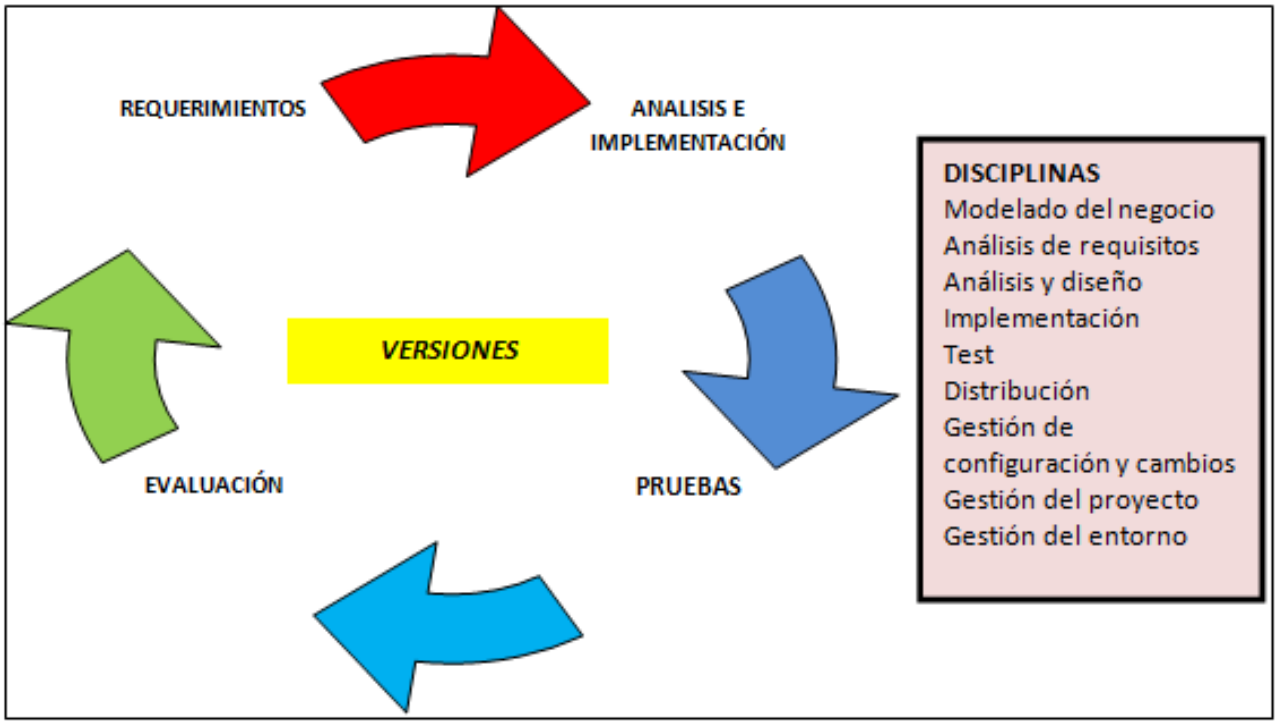
Fuente del Autor.

Metodología RUP (Rational Unified Process)

Es una metodología enfocada al desarrollo de Soluciones de Software orientado a objetos, en donde un conjunto de metodologías se pueden adaptar al contexto de la solución que requiera la organización. Una Solución con la magnitud como la que estamos planteando en este proyecto usando la metodología RUP requiere un grupo amplio de programadores. Entre las características que presenta la metodología RUP se destaca e identifica como; un marco del proyecto que describe una clase de los procesos que son iterativos e incrementales. Define un manojo entero de las actividades y de los artefactos que el proyecto necesitara para individualizarlo. RUP es el proceso de desarrollo más general de los existentes actualmente. También se basa en las mejores prácticas que se han probado en diferentes desarrollo, ofreciendo así amplias ventajas para evitar el colapso del desarrollo como podría ocurrir en la Programación Extrema (XP).

Las Fases que se deben desprender en el proyecto usando esta metodología deben ser la de Inicio, en donde se definirá el alcance del proyecto, Elaboración (Definición análisis y diseño), Construcción (Implementación) y Transición (Fin del Proyecto y entrada en Producción). Estas 4 fases deben ser planeadas teniendo en cuenta la asignación de tiempos, hitos principales resultantes, Iteración por Fases y el plan de proyecto.

Figura 5. Metodología RUP fases y disciplinas.

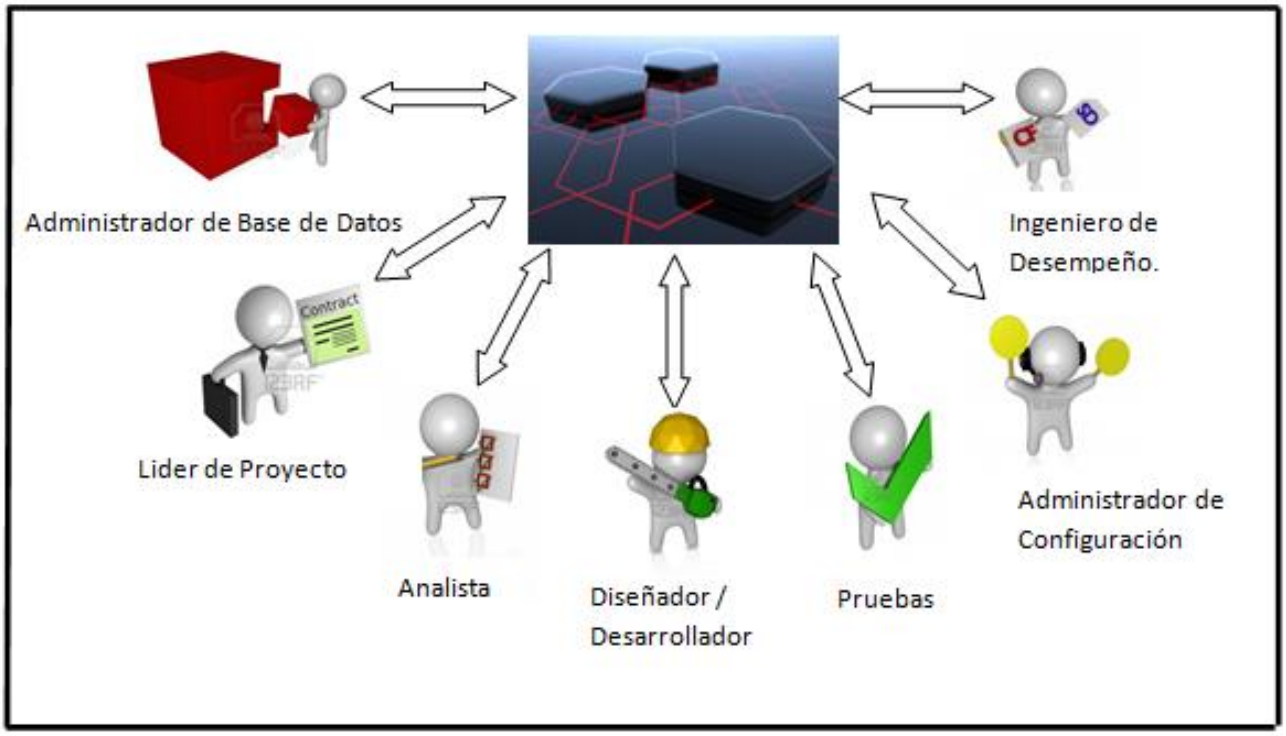


Fuente del Autor.

Los roles de los actores del proyecto también deben definirse con precisión y se debe tener claro que cada subproducto que sea generado por cada actor en su Rol especifico en el proyecto se conoce como artefacto.

Los Actores del proyecto deben compartir: Base del Conocimiento, El Proceso, Vista de Desarrollo de Software, y el Lenguaje de Modelamiento.

Figura 6. Actores del Proyecto y sus Roles (Metodología RUP)



Fuente del Autor.

En los roles definidos en la Figura 6, Se abarca cada perfil y la totalidad de los actores principales para la puesta en marcha del desarrollo de la Aplicación. La cantidad de personas con estas funciones definidas allí, pueden variar según los tiempos estipulados para la entrega y la complejidad de los procesos a automatizar.

Estándar de Seguridad de Datos para la Industria de Tarjetas

Se ha considerado importante, abordar extensamente en los lineamientos para la estructuración del proyecto de la Cedula Militar Inteligente el Estándar de Seguridad de Datos para la Industria de Tarjetas de pago, aplicando la normatividad, secciones y requerimientos que exige la Norma PCI-DSS, con la diferencia que en este proyecto no habrá pagos ni transferencias

de dinero pero se ha considerado conveniente darle una relevancia similar a las transacciones que se van a generar, ya que se estarán transportando información Sensible del Ministerio de Defensa y por consiguiente información de manejo de la Seguridad Nacional del país.

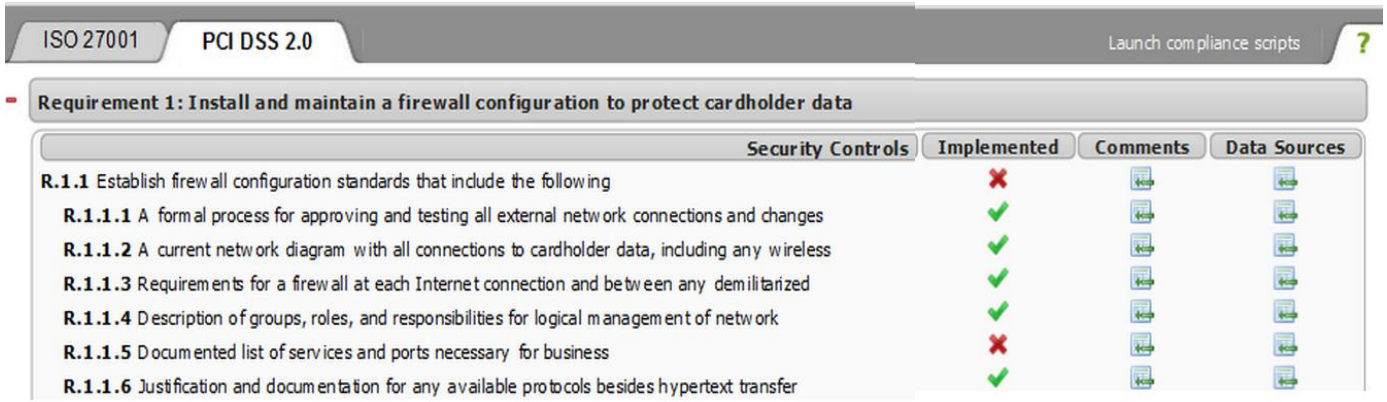
Figura 7. Secciones y requerimientos PCI DSS

Fuente del Autor.

Por la complejidad de la solución planteada y por el alcance proyectado del, es necesario se involucraren aspectos de seguridad de tipo transaccional. La solución en general con todos los procesos inmersos es en definitiva una solución de seguridad Física para la guarnición en la que se instale, para la F.F.M.M así como para el ministerio de Defensa Nacional, La seguridad Electrónica es la base operativa de la solución por la interacción de bloques de entrada, bloques de proceso y bloques de salida en un control de acceso on-line de alto dimensionamiento. Por último la seguridad informática debe ser establecida y garante en la integridad, confidencialidad y disponibilidad de la Información contenida en la operación incluyendo el tema de gestión documental Datacenter y back office.

Una manera efectiva para dar solución a los amplios requerimientos del Estándar PCI DSS, es la implementación; dentro del Segmento establecido en el esquema general de conectividad, de una Administrador de Seguridad Informática, basado en Herramientas de Código Abierto (OSSIM – Open Source Security Information Management), el cual es un Sistema de Administración y Monitorización de la Seguridad de los Sistemas de Información Corporativos basada en Software Libre y que mediante la información recibida de los distintos dispositivos internos del Sistema de control de Acceso de la red establecida, proporciona información sumarizada de todos ellos mediante "Cuadros de Mandos". Esta información proviene de todos las herramientas auxiliares instaladas.

Figura 8. INTELIGENCIA OSSIM – Mapa de Compilación Estándar PCI-DSS 2.0



Fuente. https://www.alienvault.com/

Es un Sistema de Seguridad Perimetral Integrado por más de veintidós productos relevantes en el mundo de la Seguridad y en Software Libre. Por medio de la detección, normalización, agrupación, correlación y actuación de eventos cubre de forma automática la administración de la seguridad de la Red Propuesta independientemente del tamaño y la complejidad. A través de un "pluggin" ([1]) se permite la integración con otros sistemas tantos informáticos como de seguridad.

Incorpora un Gestor de Informe, además de un Sistema de Backup, haciendo de OSSIM una herramienta que se puede calificar de integral y total en el mundo de la Seguridad. Indicar además que soporta el Análisis "Forense" que cubre gran parte de la normativa existente.

Funcionalidades OSSIM

Detectores y monitores integrados en la distribución de la solución

OSSIM entre sus amplias funcionalidades se caracteriza por la integración de Preprocesadores, Detectores y Monitores que a través de un Framework estándar de trabajo, entrega informes de tipo ejecutivo para la fácil identificación y comprensión de amenazas o Niveles de Riesgo importantes para la toma de decisiones para cualquier administrador de la Solución.

Entre los Preprocesadores mas importantes de la solución se encuentran los IDS (detectores de patrones), Detectores de Anomalías, Firewalls, Monitores Varios y Pluggins de recolección de fuentes externas

Entre las capacidades desarrolladas para aumentar la fiabilidad y sensibilidad de la detección (Posproceso), están la Correlación, Priorización y Valoración de Riesgo que hacen parte del módulo de inteligencia de la Solución.

Las Herramientas de monitorización se c aracterizan por Cuadros de Mandos (para visibilidad de alto nivel), Monitores de Riesgo y Comportamiento (para la monitorización a nivel medio) y Consola Forense y Monitores de Red (para el bajo nivel)

En los pasos a seguir en Configuración del OSSIM se tendrá que especificar en Servidor OSSIM (Consola de Gestión), en el Framework (Interacción entre Módulos), la Base de Datos centralizada de OSSIM (Interacción entre Módulos), los Agentes (Sondas Colectoras) y Todo montado sobre Sistemas Linux.

Según el alcance y las necesidades que el administrador de la solución requiera, OSSIM contiene múltiples Herramientas con servicos especializados entre los que más destacadas están; Recolección de múltiples dispositivos (Pluggins), IDS de host (Osiris), Scanner de vulnerabilidades (nessus), Inventariado servicios activo (nagios), Analizadores de protocolos (nmap), Monitor de persistencia (rrd, spade), Detección de cambios de sistema operativo (p0f), Detección de cambios de MAC (arpwatch), Anomalías de red por comportamiento (spade), Anomalías y detección de nuevos servicios (pads), Monitorización de tráfico de red (ntop), IDS (snort).

Existen diferentes Razones por las que OSSIM es una herramienta imprescindible para el responsable de seguridad informática, e indispensable para la operación que se debe ejercer en el Proyecto y soporte tecnológico de la Solución de la cedula Militar Inteligente; por eso podemos enumerar las siguientes Características a tener en cuenta.

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA CEDULA MILITAR INTELIGENTE DE LAS F.F.M.M.

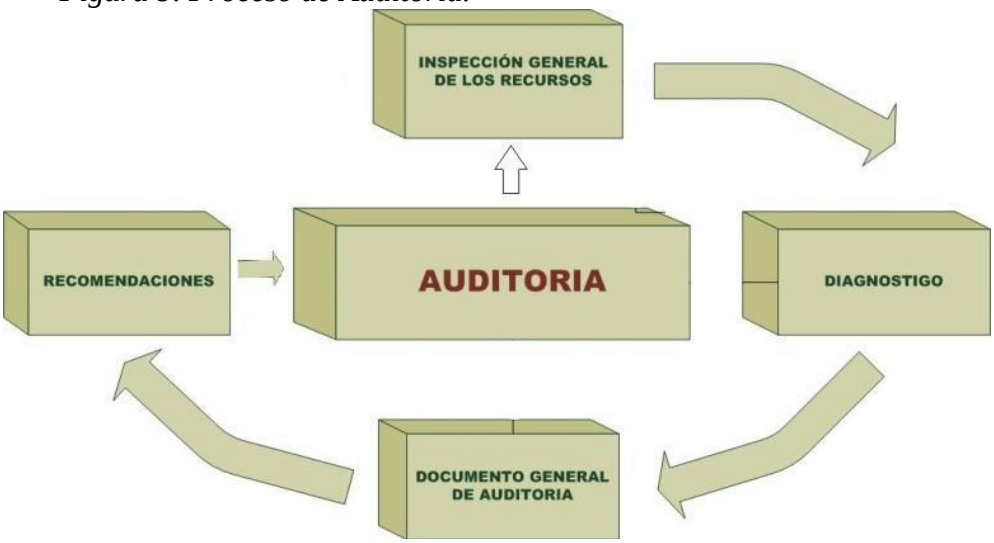
1. Plataforma de Seguridad OPEN SOURCE compuesta por más de 22 Herramientas significativas en el campo de la Seguridad Informática y soporte de administración de Seguridad adecuado para la dimensión de la Solución y la Arquitectura planteada.
2. Permite detectar y caracterizar un ataque a la Plataforma en General.
3. Dar soporte multiplataforma y multinivel, de fácil identificación.
4. La solución debe estar visualizada en Alta disponibilidad y continuidad, y OSSIM lo permite.
5. Toda información que se recibe y procesa se encuentra en formato natural y firmado asegurando su disponibilidad.
6. Disponibilidad de la información para la toma de decisiones Técnicas, Gerenciales, tácticas u Operativas.
7. Mejora del rendimiento de redes, Situación que naturalmente es crítica por el tamaño y nivel transaccional de la solución
8. Optimización de la productividad del equipo técnico de las F.F.M:M, o de la empresa integradora del soporte en general.
9. La monitorización de los eventos en Tiempo Real y la gestión de los Logs de los componentes son esenciales en la solución que tendrá enfoque IRA (Incidencia-Riesgo-Acción).
10. OSSIM es un sistema que responde a la incidencia, pudiendo determinar “Qué está pasando” “hemos encontrado el problema” “se ha resuelto el problema” , Estrategia clave para en un desarrollo con múltiples procesos e interacción de diferentes artefactos.

11. Posibilitara la gestión de riesgos y la cobertura de las diferentes normativas, tales como ISO 27000, SQX y PCI – DSS, muchos requisitos de Leyes y de normas voluntarias tipo LOPD, ISO- 27001, ISO 27002 y OSI 27005.
12. Finalmente contara Potente Cuadros de Mando y Generador de Informes para la toma de decisiones

Lineamientos para una óptima implementación de la plataforma SIM

El proceso de Auditoria Inicia con la Inspección General de los Recursos, que permitirá la ejecución de un diagnóstico preciso plasmado en un Documento General con las recomendaciones necesarias requeridas en la Evaluación.

Figura 9. Proceso de Auditoria.



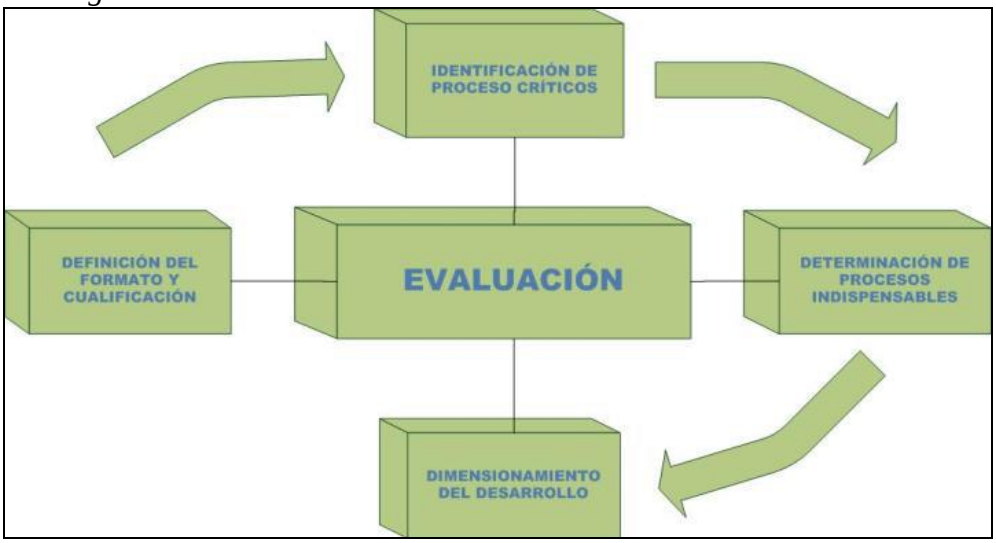
Fuente del Autor.

La auditoría debe arrojar como resultado un informe detallado que determine el alcance del módulo encargado de la Administración de la Seguridad Informática, para la red Segura a

Administrar y un anexo explícito de las recomendaciones necesarias para la puesta en marcha de dicho modulo.

Antes de empezar la evaluación debe estar definido un formato que pondere claramente todos y cada uno de los recursos de la Solución, y según esa calificación, se deben identificar los procesos Críticos que pueden comprometer la Operación y de la mano deben aparecer aquellos que indispensables para el Core del Negocio,

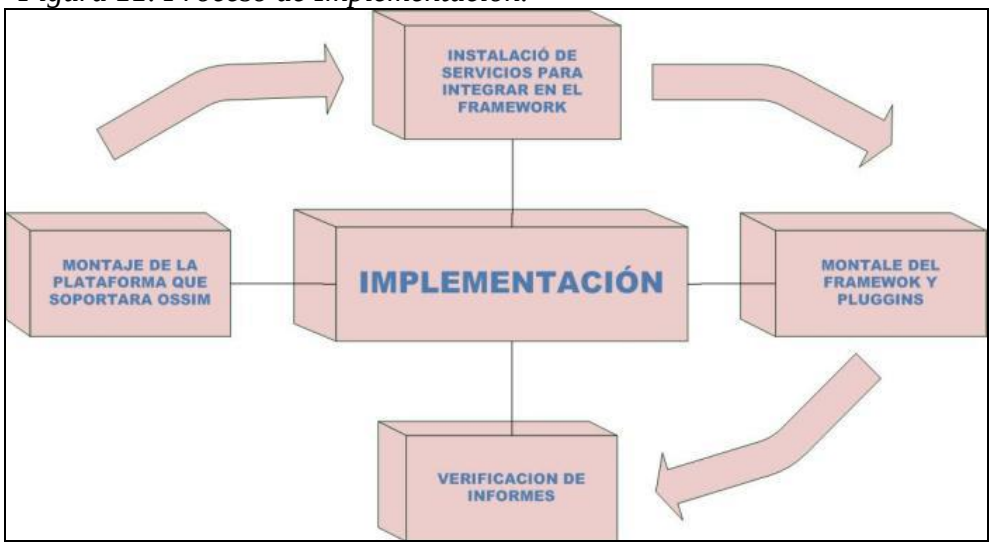
Figura 10. Proceso de Evaluación.



Fuente del Autor.

En la Segunda fase de la ejecución del módulo, y después del seguimiento de las recomendaciones generadas de la auditoria previa, se debe realizar una evaluación exhaustiva del proceso general de la Solución, y de esta manera identificar claramente los recursos informáticos involucrados en el soporte de los procesos críticos y de alta relevancia para la continuidad del negocio.

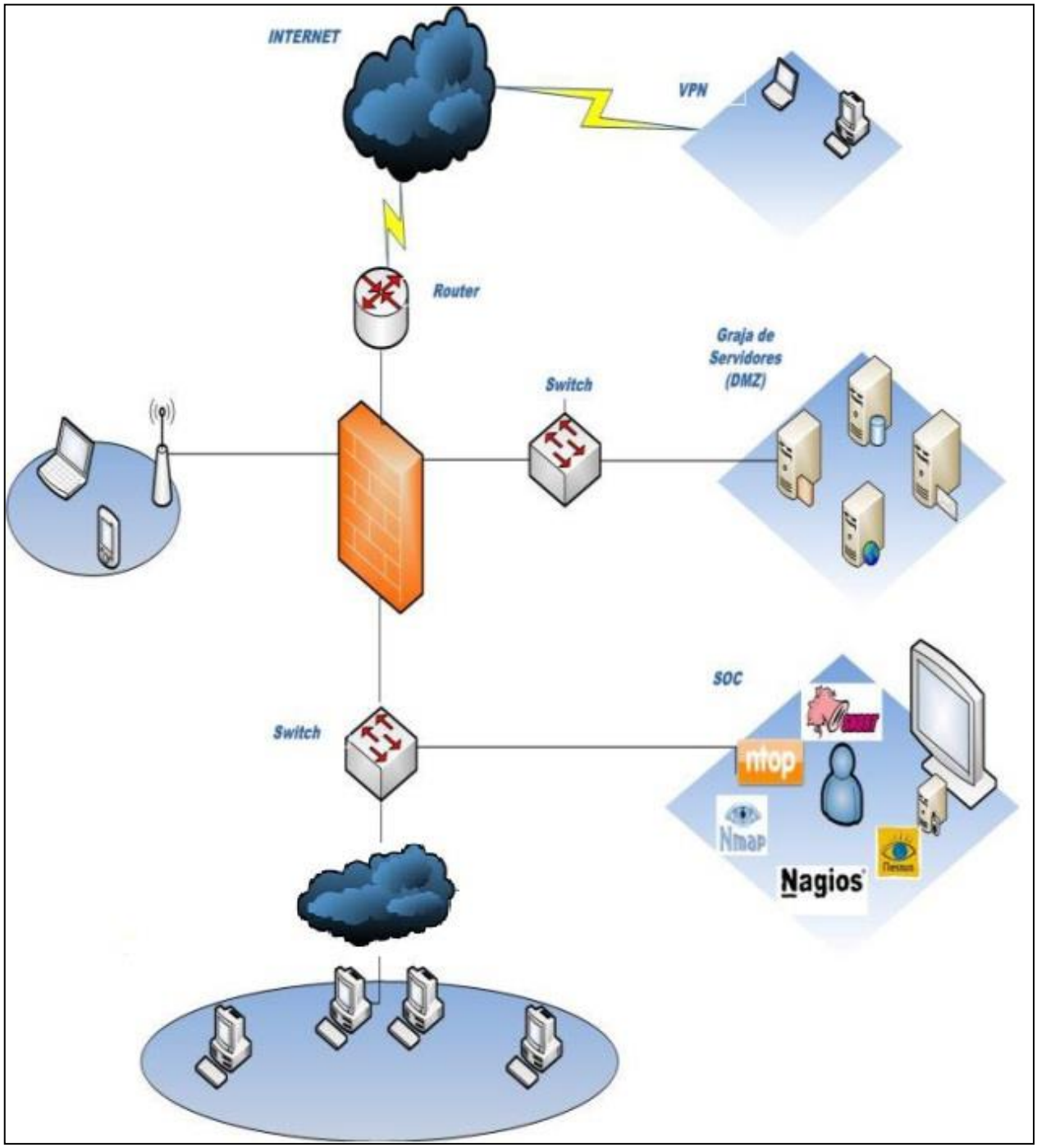
Figura 11. Proceso de Implementación.



Fuente del Autor.

Después de la Identificación de los procesos críticos que soportan el proyecto y de los recursos informáticos que los sustentan, se procede a la Implementación de la Plataforma o Modulo de Administración de Seguridad Informática del Proyecto de la Cedula Inteligente, que; a partir herramientas de Código Abierto; integrará y correlacionará las variables establecidas en la configuración del Framework y con la ayuda de informes detallados se convertirá en una herramienta colaborativa para la toma de acciones de tipo preventivo y/o correctivo que dará una facilidad en la administración de los recursos informáticos para el proyecto y así tratar de garantizar en mejor medida la Disponibilidad, Integridad y Confiabilidad de la Información, tres pilares que son la base de la Seguridad Informática.

Figura 12. Esquema de red Seguro para la Red del Proyecto.



Fuente del Autor.

La gran diferencia entre la implementación de un control de acceso convencional de altas características y la puesta en marcha del proyecto innovador propuesto en este documento, es la gran cantidad de información que se pretende gestionar, administrar y almacenar, de manera que le dará a la operación una serie de posibilidades de alto nivel administrativo y operativo para la toma de decisiones, creación de políticas y ordenamientos operacionales que a través de informes de tipo gerencial, se convierta en una herramienta versátil y eficiente que cambiara el concepto de control de acceso en las guarniciones militares de la región. Todo esto será posible por la interacción en la gestión documental del Contac Center, el Back office, el Data center, en procesos de información claramente definidos y específicos.

Conclusiones

La implementación de la Cedula Militar Inteligente para las F.F.M.M en los esquemas de seguridad Perimetral de las instituciones adscritas al Ministerio de Defensa, es una oportunidad de mejora Única que permitirá la Gestión de diferentes riesgos, y aumentara en gran medida la seguridad y el control institucional.

Una solución de altas especificaciones como la Cedula Militar Inteligente, debe ser desarrollada bajo altos parámetros de ingeniería, en los cuales toman alta relevancia la especificación del análisis diseño y desarrollo con metodología acorde como la RUP, certificaciones como PCI-DSS, Arquitecturas de Red eficientes Cliente Servidor, Administradores de Seguridad Informática como OSSIM y Políticas de Gestión Documental de alto alcance.

La visión integral del concepto de Seguridad en los controles de acceso, debe incluir necesariamente, aplicaciones y desarrollos que cubran el espectro de la Seguridad Electrónica, Física e Informática y de la información, que involucradas e interrelacionadas entre sí, generaran soluciones acordes a las necesidades de la situación Actual del país.

Es preocupante encontrar en la actualidad, aun después de hechos catastróficos ocurridos en diferentes unidades militares; no existan aun sistemas de protección desarrollados a la medida y con los alcances necesarios que requiere la Defensa Nacional y como se plantean claramente en este documento.

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA CEDULA MILITAR INTELIGENTE DE LAS F.F.M.M.

Bibliográfica

LPS Software & soluciones TI, (2008). Santiago de Compostela (A Coruña). Recuperado de http://www.lps.com.es/index.php?carga=servicios_chip

Information Quality Copyright ©, (2013). Bogotá – Colombia. Recuperado de http://www.iqcol.com/services-pci.html

PCI Security Standards Council, LLC, (2006-2013). 401 Edgewater Place Suite 600 Wakefield, MA USA 01880. Recuperado de https://www.pcisecuritystandards.org/security_standards/

Security A(r)tWork & S2 GRUPO, (2013). Cll Ramiro de Maeztu, 7 bajo, 46022 Valencia (España). Recuperado de

http://www.securityartwork.es/2013/01/02/normas-de-seguridad-pci-dss-pa-dss-y-pci-pts/

Secretaría General del Consejo de la Unión Europea (SGC) Dirección General de Justicia y Asuntos de Interior CONSEJO de la UE de Seguridad de los Documentos, DG D 1A Rue de la Loi 175 1048 Bruselas, Bélgica, (2003-2013)

http://prado.consilium.europa.eu/es/glossarypopup.html

Organización Alienvault Headquarters 1875 S. Grant Street, Suite 200 San Mateo, CA, USA 94402, (2003-2013). Recuperado de http://alienvault.com/docs/Installation_Guide.pdf

Universidad San Martin de Porres, Ciudad Universitaria Av. Las Calandrias s/n Santa Anita, Lima – Perú, (2013). Recuperado de http://www.usmp.edu.pe/publicaciones/boletin/fia/info49/articulos/RUP%20vs.%20XP.pdf

Softeng Software e Ingeniería, Av. del Doctor Arce, 14 - 28002 Madrid | España (1997-2009). Recuperado de http://www.softeng.es/es-es/empresa/metodologias-de-trabajo/metodologia-scrum.html

(1) *Open Source Security Information Management (OSSIM)*. http://www.alienvault.com/docs/AlienVault%20Building%20Collector%20Plugins.pdf