compAS
Grupo de Capacitación e Investigación pedagógica

LA SEGURIDAD FÍSICA AUTOMATIZADA EN LA ARMADA DEL ECUADOR

LA SEGURIDAD
FÍSICA AUTOMATIZADA
EN LA ARMADA DEL ECUADOR

PRIMERA EDICIÓN

Autores

Cecibel León Arreaga
Jorge Misael Merchán Riera
Patricia Marcillo Sánchez
Johanna Zumba Gamboa

Primera edición
julio 2017

Libro sometido a revisión de pares académicos.
Edición
Diagramación
Diseño
Publicación

compAS
Grupo de Capacitación e Investigación pedagógica

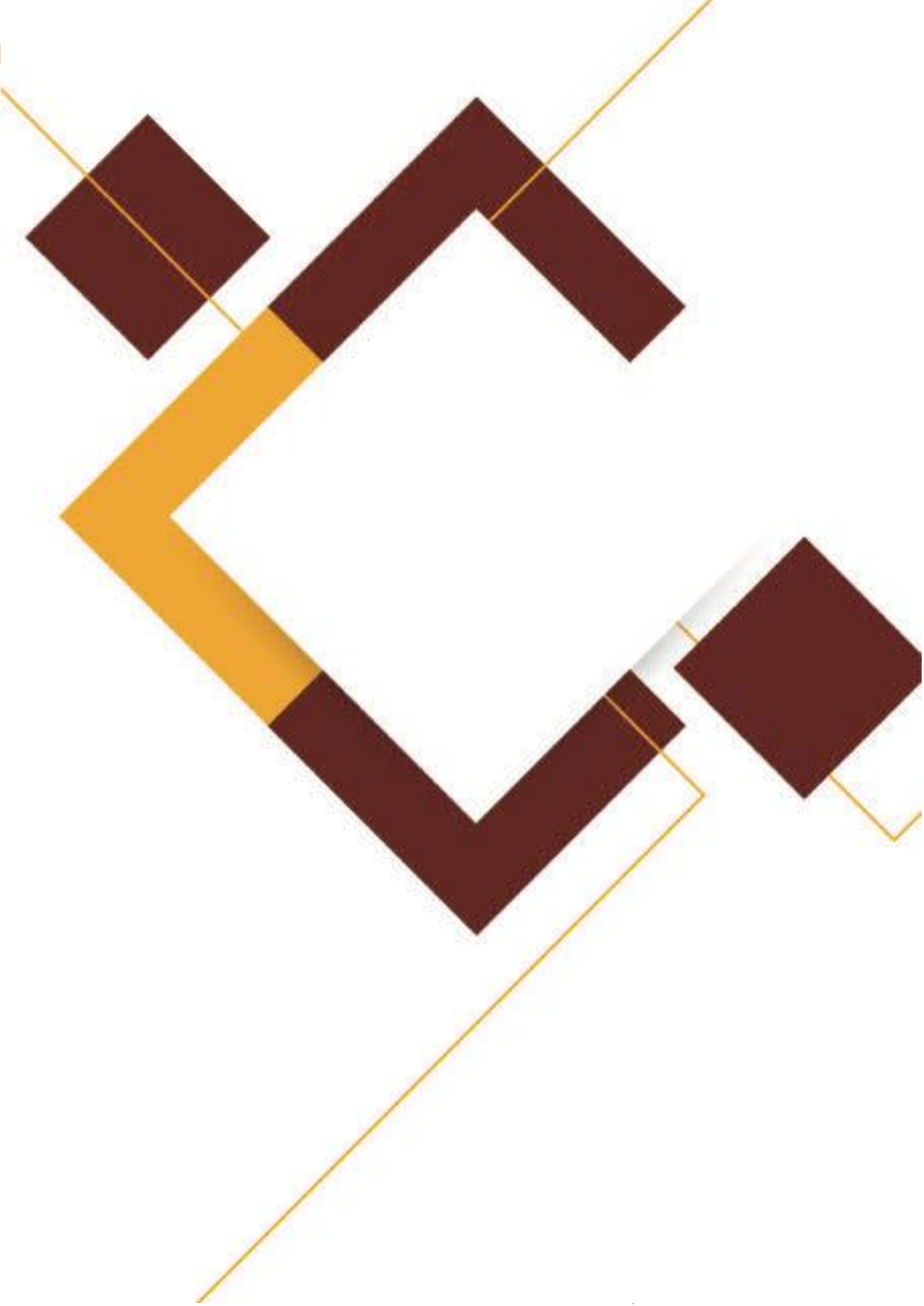
Maquetación.
Grupo Compás
Cámara Ecuatoriana del Libro - ISBN-E: 978-9942-760-50-0
Guayaquill - Ecuador

PRÓLOGO

El propósito de esta obra es diseñar la infraestructura técnica, administrativa y organizacional, que soporte un sistema de seguridad física en la Armada del Ecuador, y como caso específico en la DIGMAT.

Se realiza una presentación del problema encontrado en la seguridad de la Base Naval Sur, la importancia que tiene la seguridad física en la DIGMAT, y los problemas resultantes de la falta de automatización de la misma. Además de los objetivos que se desean alcanzar con la implementación de un Sistema informático de seguridad física automatizada. Luego, la autora relata una breve historia de la organización, su visión y misión; un análisis del actual estado de la infraestructura tecnológica, tanto de los procesos, software, hardware y redes, como lo concerniente a seguridad física; y un diagnóstico sobre la situación actual de la empresa, basado en el análisis efectuado.

Se definen los recursos necesarios para la implementación de un sistema de seguridad física automatizada en la Base Naval Sur, en especial en la DIGMAT, así también, las aplicaciones que podría tener éste dentro de la Intranet, con el propósito de sugerir a la DIGMAT una solución óptima, así como las mejoras que deben realizarse a nivel de procesos, hardware, software y redes, y un cronograma tentativo para la implementación de dicho sistema. Es evidente también un análisis financiero del proyecto a fin de determinar la factibilidad de la implementación del mismo. Con el cálculo del VAN, y el TIR del proyecto se determina que la aplicación del proyecto factible, es sin contar con los beneficios propios de la seguridad dentro de una institución como la Armada del Ecuador.



CAPITULO 1

Los recintos navales

Los recintos navales son lugares que adquieren cierto grado de sensibilidad por el tipo y/o categoría del material que contienen o trabajos que en él se desarrollan.

En la actualidad la Fuerza Naval cuenta con un bajo nivel de seguridad. Muchos de los controles de seguridad son manuales, como por ejemplo las bitácoras de ingreso y salida de los las personas. Si se desea conocer cuántas personas ingresaron a la Base Naval, en un día determinado, se debe contar en la bitácora el número de Personas que ingresaron, lo cual es una pérdida de tiempo, además de no ser 100% seguro.

Situaciones semejantes se presentan si se desea conocer quién ingresó por las garitas de seguridad sin vehículo. En algunos casos, no se registra en el bitácora, basta mostrar el carné para poder ingresar.

El ingreso al edificio es también registrado en la bitácora, siendo este, el caso de la mayoría. Existe un sistema biométrico que ayuda a controlar el personal, pero solo de ciertos repartos, es decir, no es obligatorio para todos.

En algunos departamentos de alto riesgo existe el control de ingreso a través de tarjeta, pero este control es para los que pueden ingresar libremente, sin embargo, para los visitantes no existe control alguno. Además, el control por tarjeta, solo existe en los departamentos que lo desean poner. Hay departamentos, tales como el informático, que no posee este tipo de seguridad.

Todos los sistemas antes mencionados están conectados a bases de datos independientes, y no existe una vinculación entre los diferentes sistemas de control de ingreso.

En cuanto a los sistemas informáticos, cada vez que un usuario cambia de funciones se le asigna nuevamente los permisos al sistema informático, con nuevo usuario y nueva clave; y, muchas veces tarda demasiado tiempo en otorgársele los permisos respectivos.

Lo ideal es contar con un sistema de seguridad tanto para el acceso físico como para los aplicativos, totalmente automatizado, y que nos brinde las facilidades de cambio de los accesos a los sistemas; logrando que los usuarios no tengan que solicitar cambios cada vez que cambian de plaza (lugar de trabajo), que no tengan que pedir permisos para cada área, sino que por su rango y funciones dentro de la institución tengan automáticamente los permisos. Y que los usuarios externos se vean obligados a ingresar sus datos en bitácora electrónica para tener un registro de quien ingresa y sale del edificio.

Marco de referencia

En la institución se han hecho varios sistemas de seguridad por lo delicado de las instalaciones, pero no se han aplicado en un 100%, además no comprenden una automatización integrada de todas las áreas de trabajo, sino soluciones individuales.

En el año 2003 se dieron a cabo varios acontecimientos que pusieron en evidencia la falta de seguridad que tenían las Fuerzas Armadas, y por ende, la necesidad de desarrollar un sistema automatizado para la seguridad.

Debido a esto se realizó un estudio que estuvo a cargo de cada uno de los directores de los Direcciones Navales.

En el caso de la DIGMAT, el director designó a un grupo de Oficiales para el desarrollo de un proyecto. Dentro de este grupo se encontraban varios informáticos y personal de

alto conocimiento de Seguridad, los mismos que desarrollaron un proyecto para la automatización de la seguridad.

El proyecto hacía referencia a cambios en las guardias que hace el personal. Un sistema automatizado de vigilancia que ayudaría en la prevención de las amenazas internas y externas.

Algunas de las recomendaciones que se dieron en aquel informe y en el proyecto propuesto, se llevaron a cabo, pero de manera aislada, no contribuyendo a un sistema integrado.

Entre las mejoras se menciona: las cámaras de vigilancia, los cambios en las guardias, tarjetas de ingreso a ciertos departamentos. En el gate principal se instalaron sensores para verificar que los vehículos no ingresen con armas u objetos peligrosos.

Se dispuso que se lleve por bitácora (manual) el listado de quien ingresa y quien sale de la institución.

En cuanto al personal, se proporcionó chalecos antibalas a quienes se encuentran en el gate principal.

Marco conceptual

Ancho de Banda.- Rango de frecuencias asignadas a un canal de transmisión. Corresponde al ancho existente entre los límites de frecuencias inferior y superior en los que la atenuación cae 3 dB.

ATM.- (Asynchronous Transfer Mode). Modo de transferencia definido para la RDSI de Banda Ancha, en el que la información se organiza en celdas de tamaño fijo (53 octetos).

Cable Módem.- Dispositivo que permite el acceso de datos a alta velocidad utilizando la red de Televisión por Cable.

CATV.- Antena común de televisión, a pesar de su traducción literal, no hace referencia a una antena colectiva de un edificio sino a la distribución de la señal de televisión por cable.

CM.- Abreviatura de Cable Módem.

CMTS.- (Sistema de Terminación del Cable Módem): Equipo que maneja el flujo de información en ambas direcciones.

DHCP.- (Dynamic Host Configuration Protocol) protocolo de configuración de host dinámico. Utiliza un protocolo de comunicaciones basado en UDP sobre IP.

Dirección IP.- Dirección numérica compuesta por cuatro cifras (de 0 a 255) decimales separadas por puntos.

DOCSIS.- Especificación de Interfaz de Datos sobre Servicios de Cable.

DSL.- (Digital Subscriber Line). Línea digital de abonado, constituyen la adaptación de las líneas de la red pública telefónica tradicionales, la RTPC o Red Telefónica Pública Conmutada, para la prestación de servicios de banda ancha.

Fibra óptica.- Es del cable de comunicación compuesto por filamentos de vidrio (u otros materiales transparentes) de pequeñísimo diámetro a través de los cuales se pueden transmitir enormes cantidades de información a largas distancias. La señal transmitida es un haz de luz láser, exclusivamente.

Firewall.- Se emplea tanto en grandes como en pequeñas redes para ofrecer seguridad frente a accesos no autorizados a la red interna.

FTP.- Protocolo de transferencia de archivos.

HFC.- (Hibrid Fiber Coaxial) es una red híbrida de fibra óptica y coaxial que se utiliza para la difusión de señales con un gran ancho de banda, desde una cabecera de red hasta los usuarios finales.

Host.- Es una máquina que publica contenido accesible a través de Internet.

IP Dinámico.- Es un IP que se obtiene de manera automática de un servidor

DHCP.- por un Router o equipo similar.

IP Fijo.- Es una dirección IP asignada manualmente a un dispositivo Ethernet.

ISP.- Proveedor de un Servicio de Internet.

LAN.- (Local Area Networks) es una red de área local para la conexión, a alta velocidad, de alta velocidad, de una serie de dispositivos (terminales, servidores, etc.), permitiendo de esta manera que compartan los recursos.

MAC Address.- Dirección física de la tarjeta de red (NIC).

MAN.- (Metropolitan Area Networks) es una red de área metropolitana que con velocidades de 150 Mbps permite transportar voz, datos y vídeo sobre distancias de hasta 50 km.

PACKETCABLE.- Conjunto de especificaciones desarrolladas para la prestación de telefonía IP sobre las redes de cable.

RDSI.- Red Digital de Servicios Integrados.

RF.- Radio Frecuencias

Servicio de Cable Módem.- Es el ofrecimiento de la capacidad para generar, adquirir, guardar, transformar, procesar, hacer y adquirir información vía el sistema de cable.

Softswitch.- Equipo destinado al manejo del servicio de telefonía IP.

TCP/IP.- Conjunto de protocolos que constituyen la base de Internet y que permiten la comunicación entre computadoras.

WAN.- (Wide Area Networks) es una red de comunicación de datos que tiene una cobertura geográfica relativamente grande.

Incidente.- Sucesos anormales, no queridos ni deseados, que se presentan de forma brusca, inesperada e imprevista y que dificultan o interrumpen la normal continuidad del trabajo sin causar daños a las personas.

Plan de prevención.- La planificación es un proceso mediante el cual se da repuesta a una serie de interrogantes:

- ¿Qué hay que hacer en materia de prevención de riesgos?

- ¿Quién es el responsable de hacerlo?
- ¿Cuándo hay que hacerlo?
- ¿Cuál es el objetivo a alcanzar?
- ¿Qué recursos hay que destinar

Planificación preventiva.-Proceso en el que se establecen: Objetivos medibles con plazos, Los medios necesarios para cumplir los objetivos, Plan de actuación (diseño de modelo, discusión, presupuesto, calendario, asignación de tareas y evaluación).

Incendio.- Un incendio es una ocurrencia de fuego no controlada que puede abrasar algo que no está destinado a quemarse. Puede afectar a estructuras y a seres vivos. La exposición a un incendio puede producir la muerte, generalmente por inhalación de humo o por desvanecimiento producido por la intoxicación y posteriormente quemaduras graves. Para que se inicie un fuego es necesario que se den conjuntamente estos tres factores: combustible, oxigeno y calor o energía de activación.

Seguridad.- Para otros usos de este término, véase seguridad.

El término seguridad proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

El Circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Televisión, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectad ores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros... Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

Aspectos metodológicos

El presente proyecto plantea los siguientes aspectos metodológicos:

Exploratorios y Descriptivos.

Estudios exploratorios

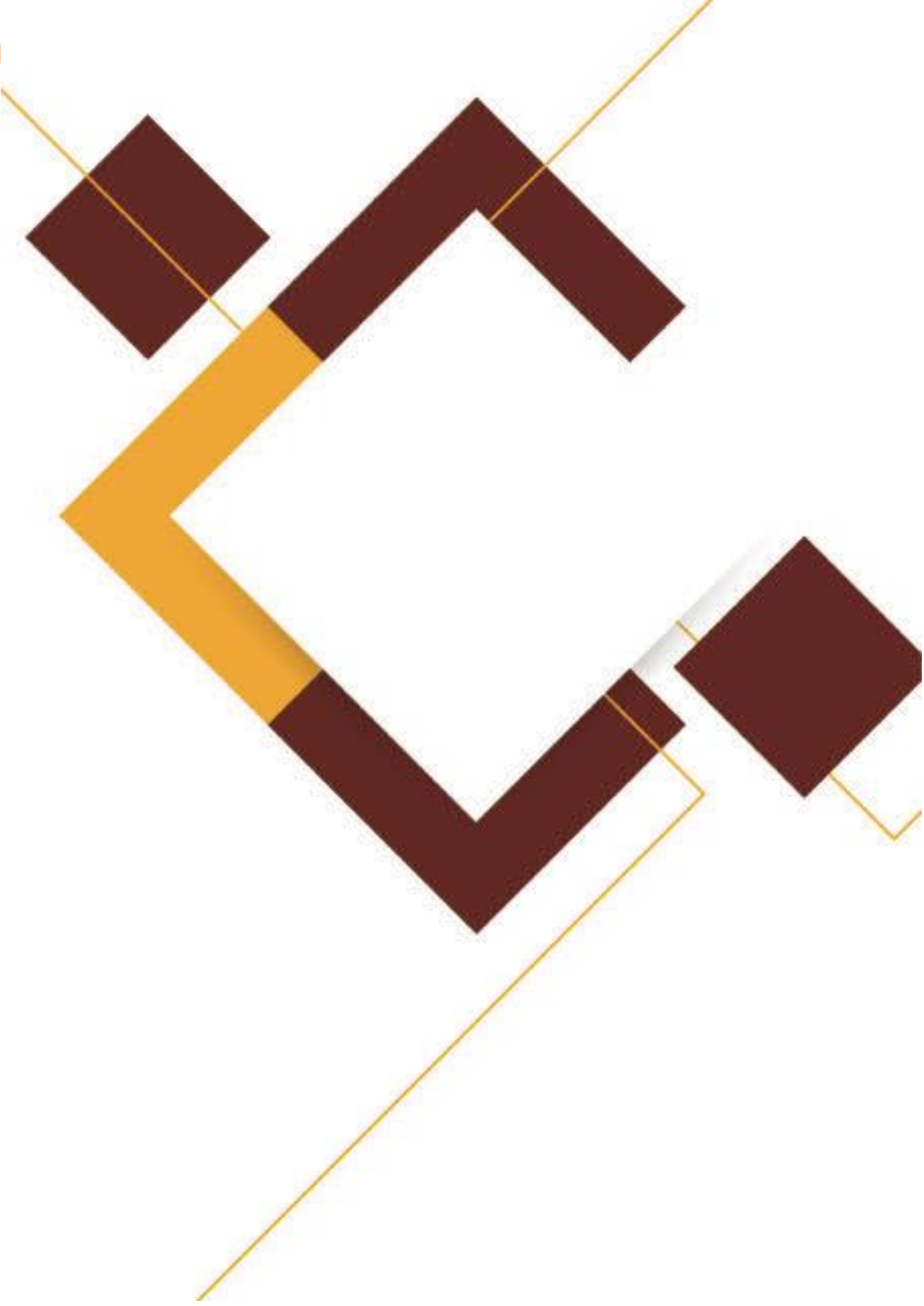
Es el primer nivel del conocimiento científico. Los estudios exploratorios sirven para aumentar el grado de familiaridad con fenómenos relativamente desconocidos. Normalmente no constituyen un fin en sí mismos sino que son el punto de partida para la realización de los otros tipos de estudios, que tienen un mayor nivel de profundidad.

Los estudios exploratorios se interesan fundamentalmente en descubrir. Ejemplo: una investigación bibliográfica sobre la administración de los recursos humanos.

Estudios descriptivos

Es el segundo nivel de "conocimiento científico". Busca especificar las propiedades y características importantes del objeto de investigación (personas, grupos o comunidades). Identifica, por ejemplo las características del universo de

investigación, señala formas de conducta, establece comportamientos concretos y determina y comprueba asociación entre variables. Los estudios descriptivos se interesan fundamentalmente en *medir*.



CAPITULO 2

Análisis de la situación actual en la armada del Ecuador

Historia

La Historia de la Armada del Ecuador se remonta a los tiempos aborígenes, pero es en la República cuando recién se le da un nombre legal:

> El 3 de noviembre de 1832, el Congreso Constitucional del Ecuador decretó que el establecimiento de la Marina Militar se llamara Departamento Marítimo del Ecuador en vez de la antigua denominación de Apostadero de Guayaquil. El 8 del mismo mes, el general Juan José Flores disponía el ejecútese. El mando de este Departamento se lo dio a un general de brigada de Marina o capitán de navío, bajo la denominación de Comandante General. Se estableció también la Mayoría de Marina dirigida por un capitán de fragata. De este modo se legalizó la Marina durante la República.

El Hecho más relevante de la Historia de la Armada en el siglo pasado fue el Combate de Jambelí en honor al cual se celebra el 25 de julio el día de la Armada del Ecuador

> **Combate Naval de Jambelí**
>
> En 1941, cuando nuestro país era víctima de una agresión territorial y el Ejército peruano penetraba por nuestras fronteras, se suscitó un episodio histórico en el mar que, por su heroísmo y magnitud, representa un legado histórico de honor.
>
> El 25 de julio, mientras las tropas defendían por tierra la heredad patria, el cañonero "Calderón" , comandado por el Teniente de Fragata Rafael Morán Valverde, enfrentó al destructor "Almirante Villar" en el canal de Jambelí. El buque peruano abrió fuego a las 11:30 horas, la contienda fue desigual por ser el destructor considerablemente superior en dimensiones, características y condiciones bélicas. Informó el Comandante Morán Valverde que la acción se sostuvo únicamente con el cañón de 3 pulgadas de proa y dos antiaéreos de 20 mm., ya que el cañón de 3 pulgadas de popa falló después del primer disparo que impactó en la popa del buque enemigo. Los disparos fueron efectivos, pues sus impactos deterioraron partes vitales del buque agresor, causando bajas en su personal, obligándolo a replegarse. El cañonero "Calderón" no sufrió daño alguno a pesar de que los piques del enemigo le pasaron muy cerca. El combate se prolongó hasta las 11:46 horas, como consta en el parte enviado por el Comandante Morán Valverde.
>
> El resultado favorable para nuestra nave de guerra se debió a la heroicidad con la que combatió la tripulación, a pesar de la deficiencia absoluta de material, ya que sólo respondió un 30% de los proyectiles y fue la pericia de los artilleros la que niveló a su favor el combate.
>
> El efecto estratégico de esta invaluable acción naval evitó que la escuadra peruana cumpliera su misión de bloquear el Golfo e interceptar los convoyes entre Guayaquil y Puerto Bolívar.. (DIRTIC, 2012)

MISIÓN

Desarrollar las capacidades marítimas y proveer la seguridad integral en los espacios acuáticos que fortalezcan el Poder Naval y que contribuyan a la defensa

de la soberanía y la integridad territorial; y, con su contingente apoyar al desarrollo marítimo nacional y a la seguridad pública y del Estado. (DIRTIC, 2013)

VISIÓN

En el año 2021, ser un Poder Naval con capacidad para el control integral y permanente del territorio marítimo en el marco de la CONVEMAR, comprometido en el desarrollo marítimo del país, con talento humano profesional y con alto sentido de pertenencia. (DIRTIC, 2013)

VALORES (DIRTIC, 2013)

- LEALTAD.
- HONOR.
- DISCIPLINA

OBJETIVOS INSTITUCIONALES

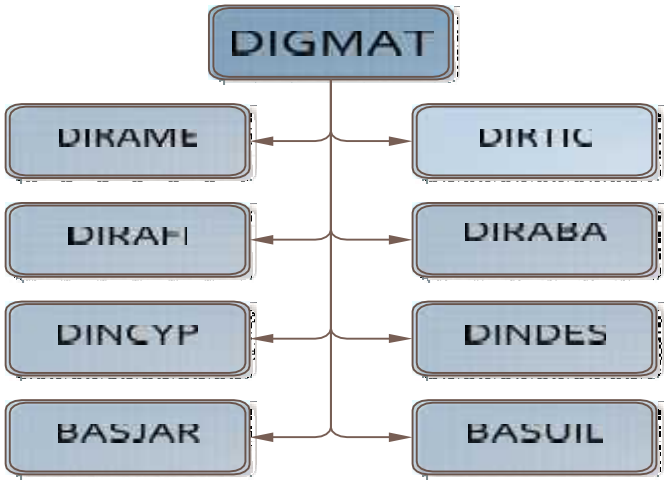
1. Incrementar la imagen, credibilidad y confianza en la Armada del Ecuador como fuerza, institución y autoridad.
2. Incrementar la participación, compromiso y ejecución en la gestión de la política y desarrollo marítimo, fluvial y antártico, con responsabilidad social y ambiental.
3. Incrementar el Apoyo a la Acción del Estado en la protección de áreas estratégicas, defensa interna y seguridad marítima en el área de competencia de la Armada.
4. Incrementar la participación institucional en operaciones de mantenimiento de paz, ayuda humanitaria y de cooperación internacional.
5. Incrementar la presencia naval en las aguas interiores y ejes fluviales, mar territorial, zona económica exclusiva continental e insular y recuperar las capacidades de vigilancia, mando y control.
6. Incrementar el alistamiento operacional de las unidades navales.
7. Incrementar las capacidades para la defensa y seguridad integral del territorio marítimo nacional.
8. Incrementar la integración y estandarización administrativa de la Armada a través de un sistema de planificación estratégica, presupuestaria, riesgos y procesos.
9. Incrementar el desarrollo y gestión del talento humano de la Armada en la formación, perfeccionamiento, capacitación, especialización por competencias y la gestión del clima laboral.
10. Incrementar la innovación e implementación de tecnologías aplicadas al campo naval.
11. Incrementar la gestión de los recursos financieros asignados a la Armada. (DIRTIC, 2013)

DIRECCIÓN GENERAL DEL MATERIAL

Como se muestra en la Figura No. 2.1 A continuación una breve descripción de la Dirección General del Material:

La Dirección General del Material (DIGMAT) y las direcciones navales que conforman el Sector del Material de la Armada, son órganos técnicos-administrativos, responsables de los procesos gobernantes de "Planificación y evaluación"; de los procesos agregadores de valor: "Mantenimiento y Recuperación de Unidades Navales y Municiones"; "Desarrollo de Bases y Repartos en Tierra" y, el de "Servicio Logístico de Bases" y de los procesos de soporte: "Adquisición de Bienes y Servicios" "Abastecimiento de bienes y servicios" y, "administrativo financiero", cuya estructura orgánica funcional es lineal, tiene las siguientes Direcciones subordinadas: Mantenimiento y Recuperación de Unidades Navales, Ingeniería Civil y Portuaria, Abastecimientos de Bienes y Servicios y la de Administración y Finanzas, responsables de las funciones logísticas de mantenimiento, abastecimiento, desarrollo de bases y transporte terrestre, creado mediante Acuerdo Ministerial No. 131 3, expedido el 28 de diciembre de 1976, publicado en la Orden General Ministerial No. 244 del 28 de diciembre de 1978 (ESPINOZA, 2008)

Organigrama de la Dirección General del Material



Fuente: (DIGMAT, 2008)
Elaborado: Dpto. Procesos de la DIGMAT

ANÁLISIS DEL PROCESO ACTUAL

Como se ha referido en el Capítulo que precede, la seguridad siempre ha sido un factor importante para La Fuerza Naval del Ecuador, pero debido a factores, en muchos casos externos no se ha logrado la automatización de la misma.

Es a partir del año 2003, cuando por acontecimientos que demostraron la vulnerabilidad de la seguridad en los diferentes repartos de La Fuerza Naval del Ecuador, cuando se empieza a dar importancia a la automatización de la seguridad en los repartos navales. Antes todo se lo llevaba manualmente, a través de bitácoras. Es entonces cuando el ESMAAR, a partir de los hechos antes mencionados, solicita a los diferentes repartos de La Fuerza Naval del Ecuador que se creen proyectos que ayuden a mejorar la seguridad. (DIGMAT, 2003)

Es así que se crean proyectos aislados en cada uno de los repartos, muchos de los cuales nunca se concluyeron, y algunos ni se empezaron. Estos proyectos carecían de profundidad, solo llevaban lo relevante y urgente, no se pensó en las nuevas instalaciones que se crearían después, quedando en poco tiempo obsoletas; luego se hicieron parches a estas soluciones, y no se vio el real enlace que tiene en la actualidad la tecnología informática con la seguridad física.

En el año 2005, el CETEIN-DIGMAT creó un proyecto que unía lo informático con la seguridad, muy bien elaborado, pero se centraba más en las seguridades del departamento en sí. Sin embargo, es digno de mencionar, porque a partir de este proyecto se han hecho varias replicaciones en otros departamentos. (DIRTIC, 2005)

Con el propósito de dar una perspectiva de cómo se encuentran los procesos de Seguridad en La Fuerza Naval Nacional se procederá a describir los procesos y determinar sus falencias.

INGRESO Y SALIDA DE PERSONAL

1. Ingreso de datos al Sistema

2. El empleado solicita el ingreso de los datos al departamento de Recursos Humanos

3. En el Departamento de Recursos Humanos se ingresan los datos del empleado al sistema Biométrico.

4. En el Departamento de Recursos Humanos se toman las huellas dactilares del empleado

5. Se almacenan los datos en un sistema que tiene una base de datos de Access.

6. En el Departamento de Recursos Humanos se entrega un código de acceso al empleado

7. El empleado recibe el código de Acceso al sistema Biométrico

Control Hora de Entrada y Salida

El empleado digita el Código de acceso, presiona la opción de entrada o salida y coloca el dedo en el Lector de Huella.

1. El sistema analiza el código y la huella dactilar, para ver si el ingreso es correcto.

2. Si el ingreso es correcto entonces almacena los datos en la base de Datos de Access.

3. Por No envía mensaje de error al usuario.

Control Hora de Entrada y Salida (otros repartos)

4. El usuario pasa la tarjeta en el dispositivo de lectura de aproximación.

5. El sistema ingresa los datos en una base de Access

Control Entrada y Salida Visitantes

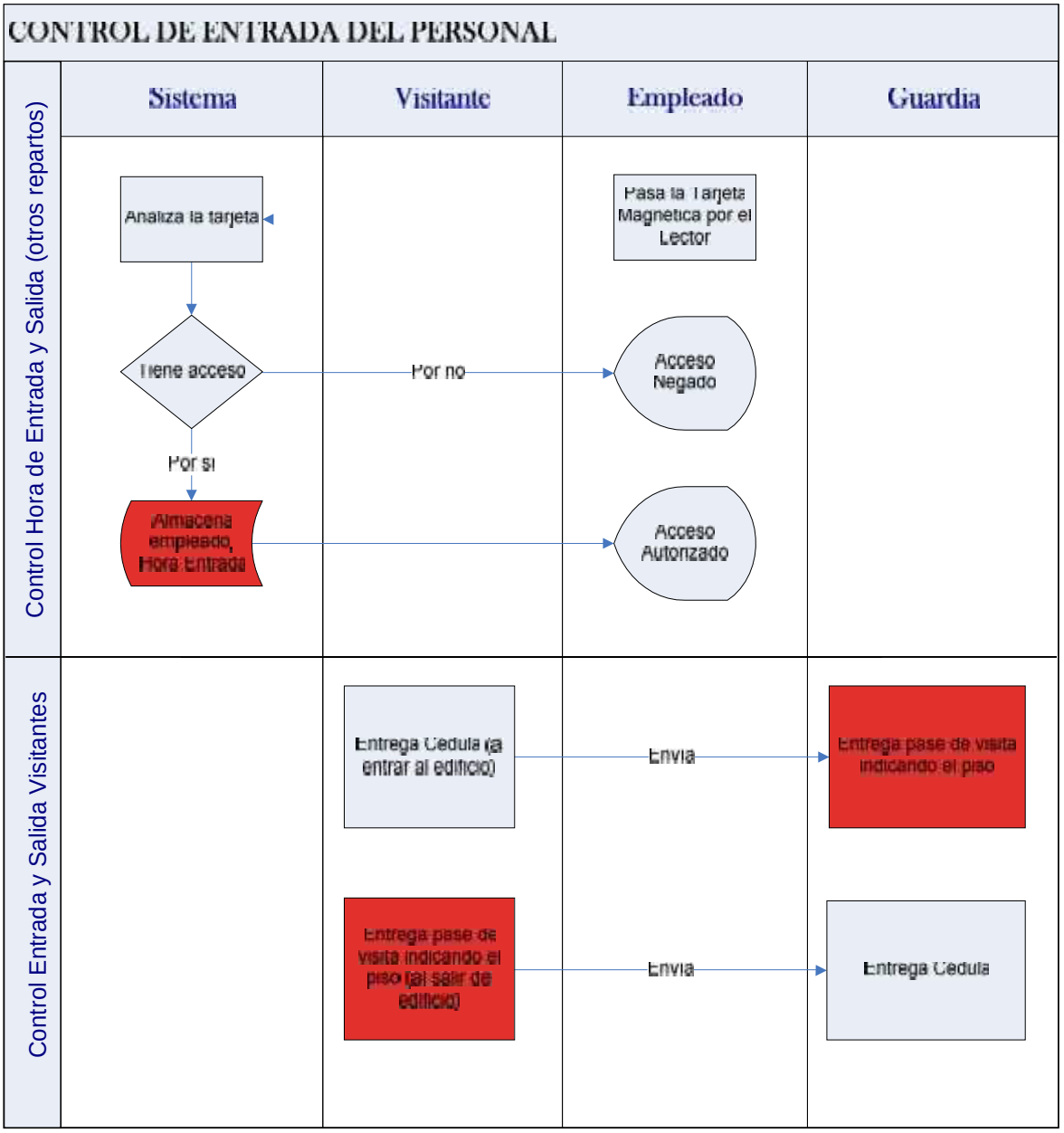
6. Entrega Cédula (al entrar al edificio)

7. El encargado de la guardia entrega el Pase de Visita indicando el piso al que tiene acceso el invitado.

8. Al salir el visitante entrega el Pase de Visita al encargado de la guardia

9. Encargado de la guardia entrega la cédula al Visitante.

Control de Entrada y Salida del personal



Fuente: (Investigación, 2012)

Elaborado por: Ing. Cecibel León Arreaga.

INGRESO A LOS SISTEMAS INFORMÁTICOS

INGRESO DE PERSONAL EN RRHH

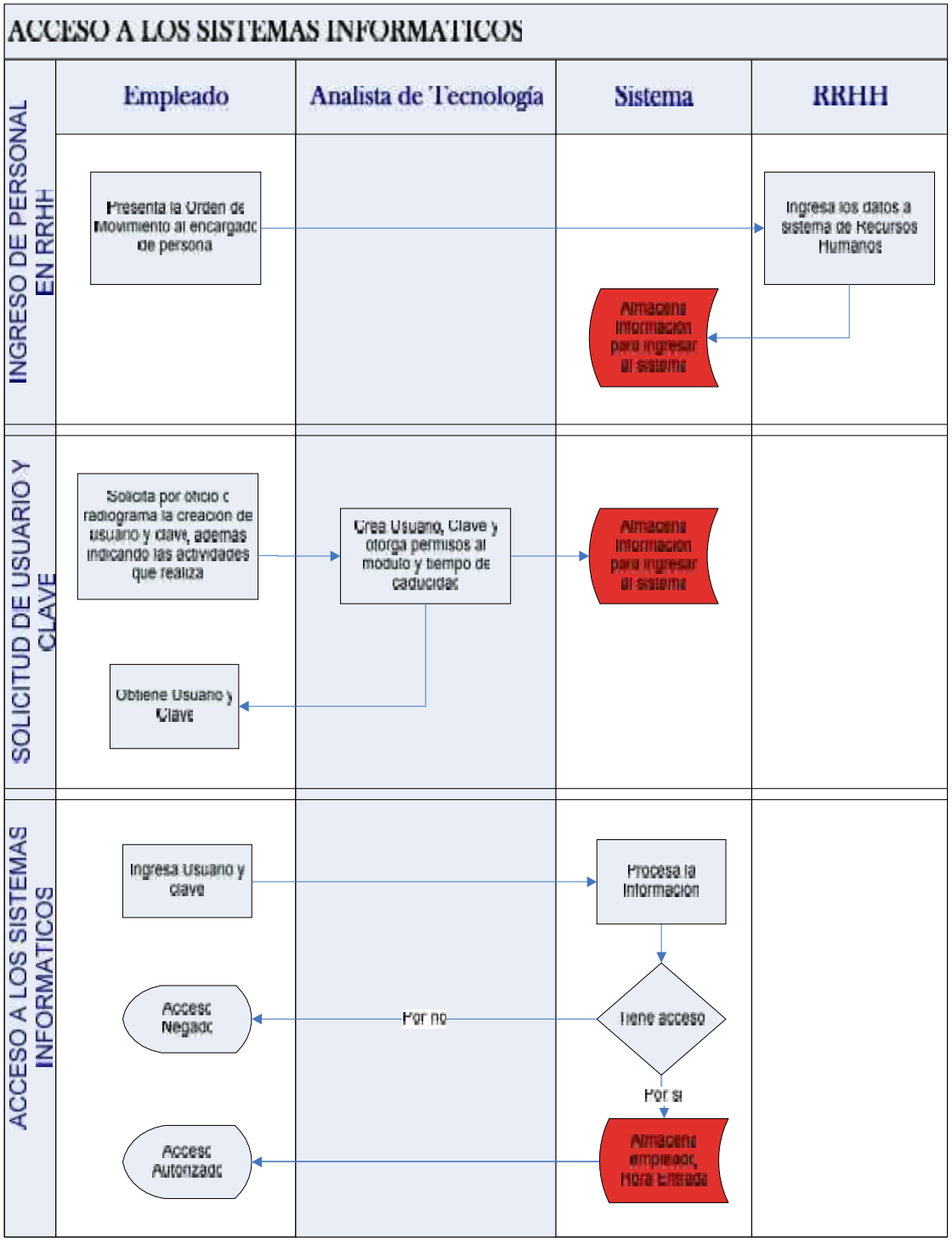
1. El empleado presenta la Orden de Movimiento al encargado de personal
2. El encargado de Recursos Humanos Ingresa los datos del empleado en el Sistema de Recursos Humanos
3. Se almacena la Información del empleado en la base de Datos de Informix del Sistema SISLOG.

SOLICITUD DE USUARIO Y CLAVE

1. Solicita por oficio o radiograma la creación de usuario y clave, además indicando las actividades que realiza
2. El Analista de Tecnología encargado, crea Usuario, Clave y otorga permisos a los módulos que requiera el usuario
3. Se almacena la Información del usuario en la base de datos de Informix del Sistema SISLOG.
4. Se entrega Usuario y Clave al empleado.

ACCESO A LOS SISTEMAS INFORMÁTICOS

1. Ingresa Usuario y Clave
2. Procesa la Información
3. Si el usuario y clave son correctos, almacena datos de Hora y Fecha de ingreso en la base de Datos de Informix del Sistema SISLOG.
4. Muestra mensaje de ingreso satisfactorio
5. Si usuario y clave son incorrectos muestra mensaje de error.

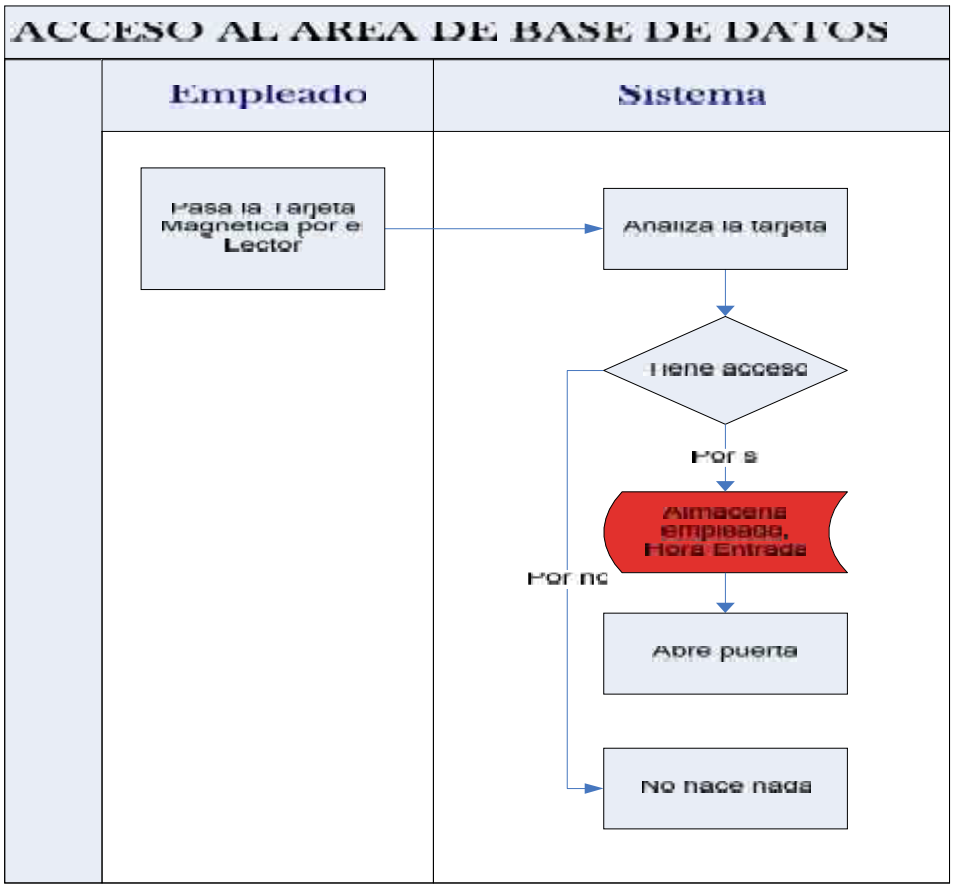


Accesos A Sistemas Informáticos

Fuente: (CETEIN-DIGMAT, 2008)

Elaborado por: Ing. Cecibel León Arreaga.

Acceso A La Base De Datos



Fuente: (Investigación, 2012)

Elaborado por: Ing. Cecibel León Arreaga.

ANÁLISIS DEL SOFTWARE

En la Fuerza Naval existen un sinnúmero de sistemas con los que se realizan la toma de los ingresos y salidas. Estos sistemas de acuerdo a la opinión de los usuarios (Ver encuesta no proporcionan mayor información, lo hacen para el control de personal que labora en las instituciones, restándole importancia a la seguridad y revisión

de ingreso y salida de personal de fuera del reparto, puesto que, como se indicó antes, estos se los ingresa en una bitácora manual, y en muchas ocasiones no se los registra. Cada reparto tiene su propia base de datos para llevar el control de acceso.

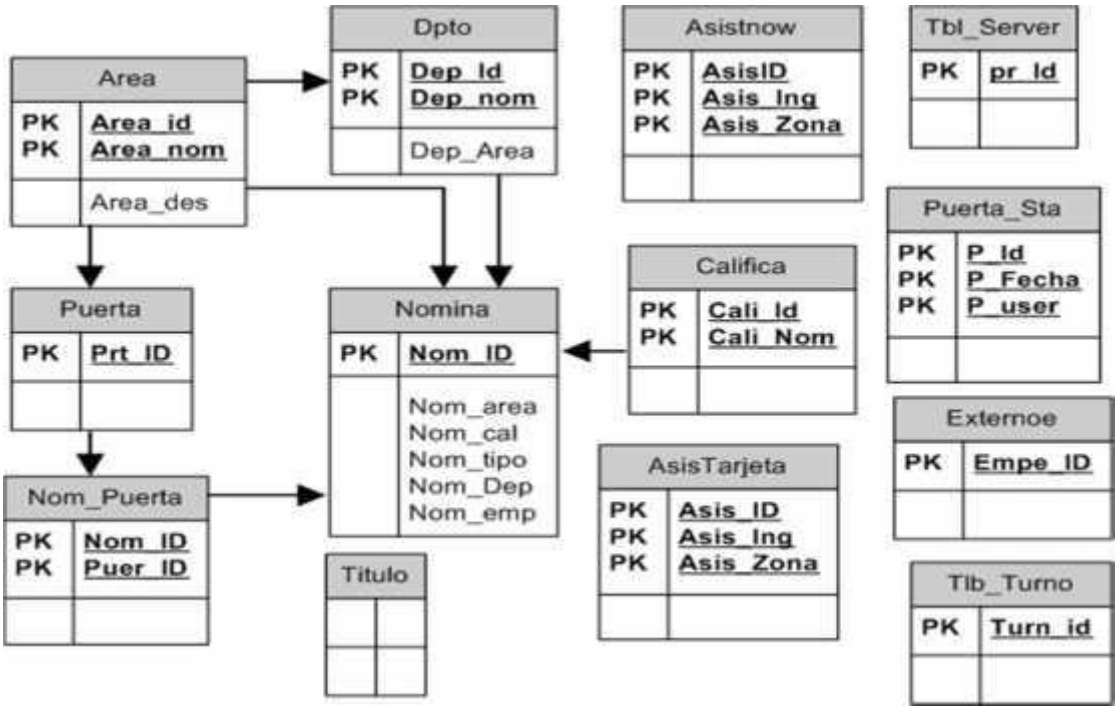
En el edificio DIGMAT-DIGREH, hay un sistema que sirve para el control biométrico a través del dedo índice, el mismo que se usa para el control de asistencia de los servidores públicos (civiles), mas este no tiene relación con la Base de datos del módulo de Recursos Humanos, es decir que, son datos aislados y no permiten la integración con los demás repartos, En caso de necesitar esos datos en otros repartos se debería tener otra base igual o un respaldo (copia) de la misma. Además se encuentra el problema de que está hecho en SQL y Visual Basic, y como se sabe, todas las entidades públicas deben tener sus sistemas en software open source, lo que implica que debe ser migrado.

BASE DE DATOS DEL SISTEMA BIOMÉTRICO DE DIGMAT

La Base de Datos del sistema biométrico se encuentra en una máquina, no en un servidor, además se encuentra fuera del área de servidores de la DIGMAT. Los respaldos los realiza la única persona que tiene acceso al sistema, por no ser experto no hace comprobaciones de la base. El administrador de base de datos, toma estos respaldos, pero no se siguen procedimientos de comprobación de los mismos, ni se hacen respaldos en otros lugares por considerarlo una aplicación sin mayor importancia.

A continuación se muestra un modelo entidad-relación del mismo, y una breve descripción de las principales tablas.

Modelo Entidad Relación de la Base de Datos del Sistema Biométrico de la DIGMAT



Fuente: Diccionario de Datos - Modelo Entidad Relación (ONLYCONTROL, 2010)
Autor: Only Control S.A.

PRINCIPALES PANTALLAS DEL SISTEMA BIOMÉTRICO DE DIGMAT

Pantalla de Acceso al Sistema

La primera pantalla es la de control de acceso en la cual el usuario ingresa su código y pone su huella para acceder al sistema Biométrico de la DIGMAT, a esta pantalla solo tienen acceso los un usuarios que administran el sistema o que tienen permisos para sacar los reportes.

Pantalla de acceso al sistema

Fuente: Sistema Biométrico de la DIGMAT (Only Control S.A., 2010)

Autor: Only Control S.A.

Pantalla Principal o de Menú

La Pantalla principal del sistema, muestra las diferentes opciones que tiene el sistema.

Pantalla Principal

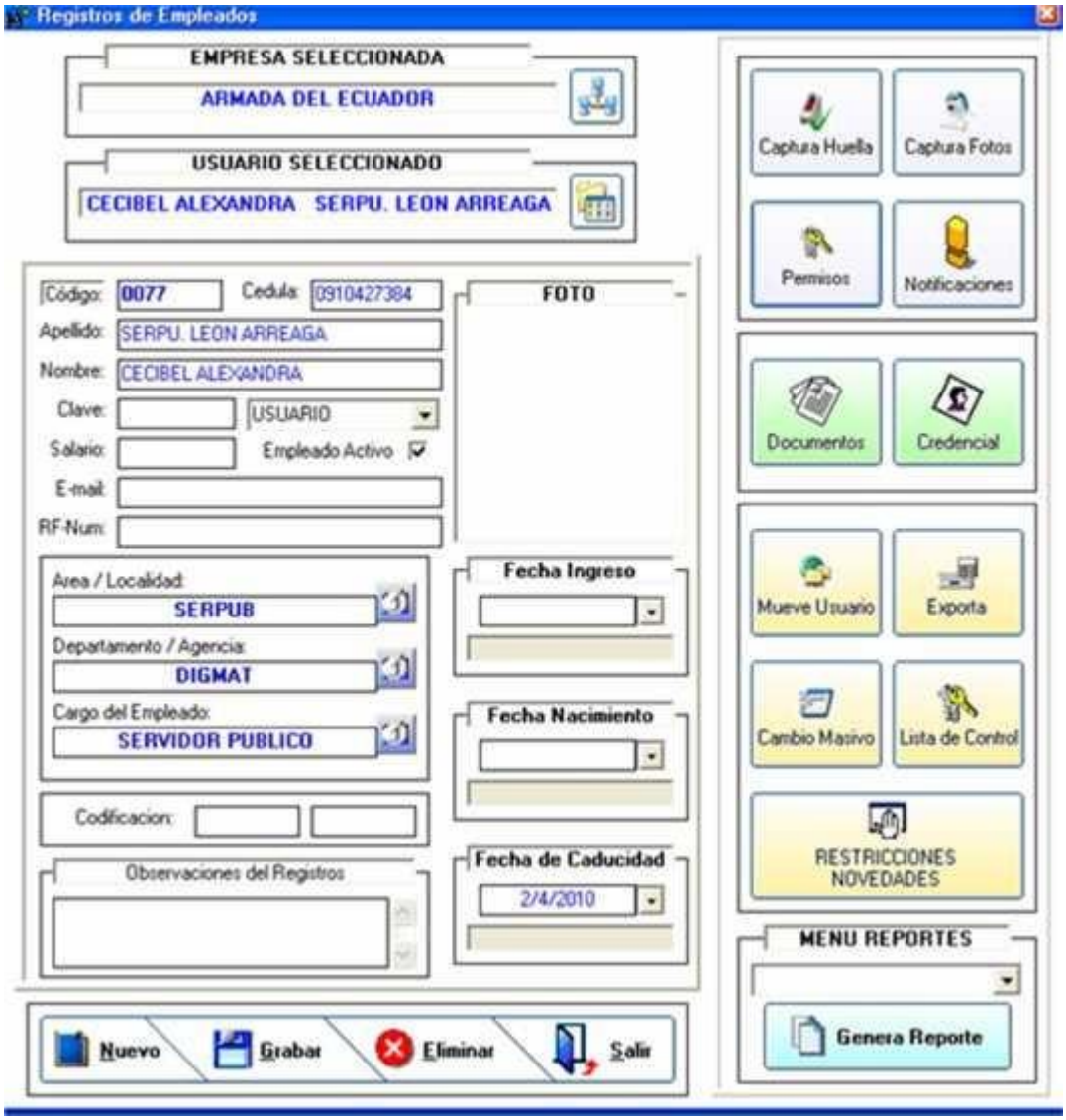
Fuente: Sistema Biométrico de la DIGMAT (Only Control S.A., 2010)

Autor: Only Control S.A.

Pantalla de Ingreso del Personal

Pantalla de ingreso de personal: en la siguiente pantalla se ingresan los datos de los empleados de la DIGMAT, como podemos observar los principales datos son código, apellido, nombre, clave, salario, e-mail, número de una referencia, área, departamento, cargo, fecha de ingreso, fecha de nacimiento, fecha de caducidad, se captura la huella, se captura la foto, se da permisos según horarios preestablecidos, etc.

Registro de Empleados



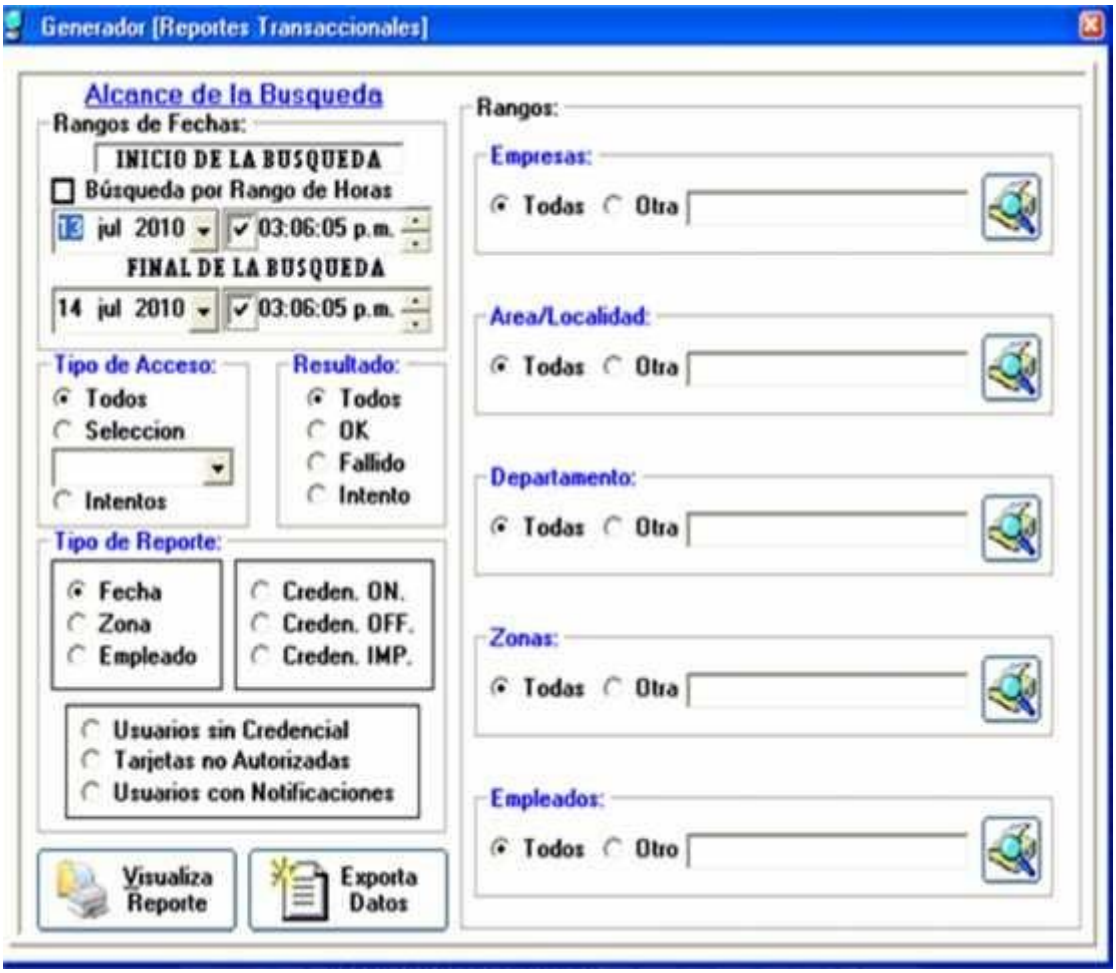
Fuente: Sistema Biométrico de la DIGMAT (Only Control S.A., 2010)

Autor: Only Control S.A.

Pantalla de Reportes

Pantalla de Reportes: en esta pantalla se ven las diferentes opciones por las cuales se puede filtrar los datos del Ingreso y Salida del personal, como: fechas, empresa, localidad, departamento, zonas, empleados, tipo de accesos, resultados, y otros, lo que facilita la emisión de los reportes.

Pantalla de Reportes

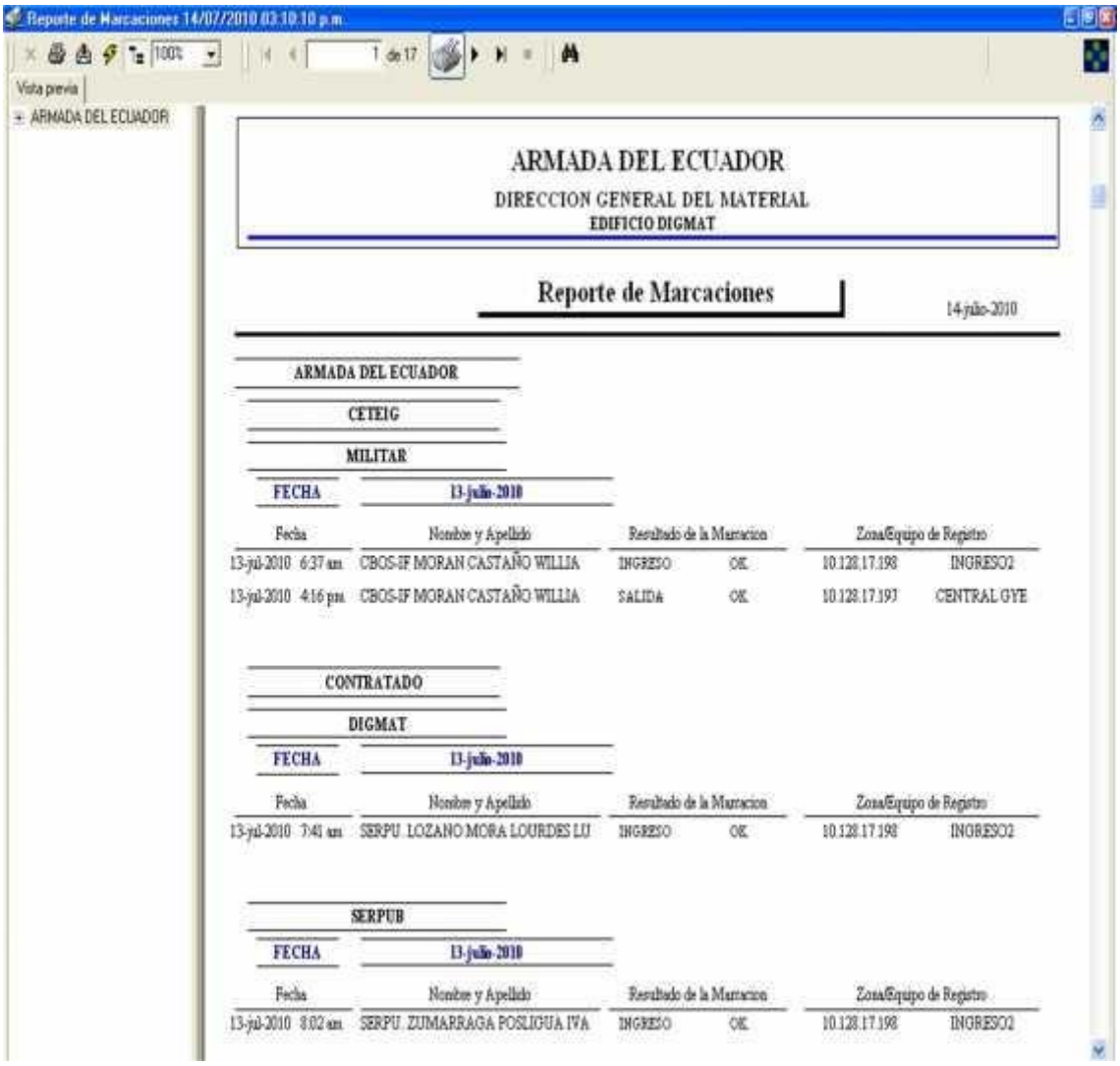


Fuente: Sistema Biométrico de la DIGMAT (Only Control S.A., 2010)

Autor: Only Control S.A.

A continuación un ejemplo de los reportes que se pueden obtener del sistema.

Reporte de Marcaciones del personal



Fuente: Sistema Biométrico de la DIGMAT (Only Control S.A., 2010)

Autor: Only Control S.A.

ANÁLISIS DEL HARDWARE

El hardware lo podemos dividir en 2 partes: el Hardware del sistema Biométrico y el hardware de seguridad, tal como cámaras digitales, etc.

HARDWARE DEL SISTEMA BIOMÉTRICO

El hardware consiste en un equipo de huellas digitales, como se se muestra en el gráfico

Equipo De Huellas Digitales

Fuente: Manual Access Control (CETEIN-DIGMAT, 2010)
Autor: CETEIN-DIGMAT

La base de datos no se encuentra en un servidor, está en un PC de las siguientes características:

Procesador:	Inter Corel 2 Duo
Disco duro:	350 GB
Sistema Operativo:	Windows XP server
Memoria RAM	2 GB

En cuanto a las cámaras y demás equipo de vigilancia, se tiene lo siguiente:

En el edifico DIGMAT-DIGREH existe un sistema de circuito cerrado de cámaras de seguridad, las mismas que se encuentran localizadas de la siguiente manera:

- 2 Cámaras de Vigilancia en las esquinas opuestas de los corredores de cada piso, las mismas que tienen sensor de movimiento. En planta baja, y del primero al quinto piso, en total 12 cámaras. (Indoor Cameras(MGS-BT-176WC-DN) 12 Color)
- 4 cámaras de vigilancia de alto alcance que cubren los alrededores del edificio cada una a un lado del edificio en la planta baja. (Outdoor Cameras(MGS-DC-222WC) 4 Color)
- DVR de 120/60 fps
- Cámara Bullet a Color Dia/Noche con Tecnología Infrarroja
- Mini Domo con Chip Sony a Color de Alta Calidad
- 100' de cable Plug & Play
- Monitor a color de 20" Color Monitor (Digital Video Recorder 16 Channel Monitor 20" Color)

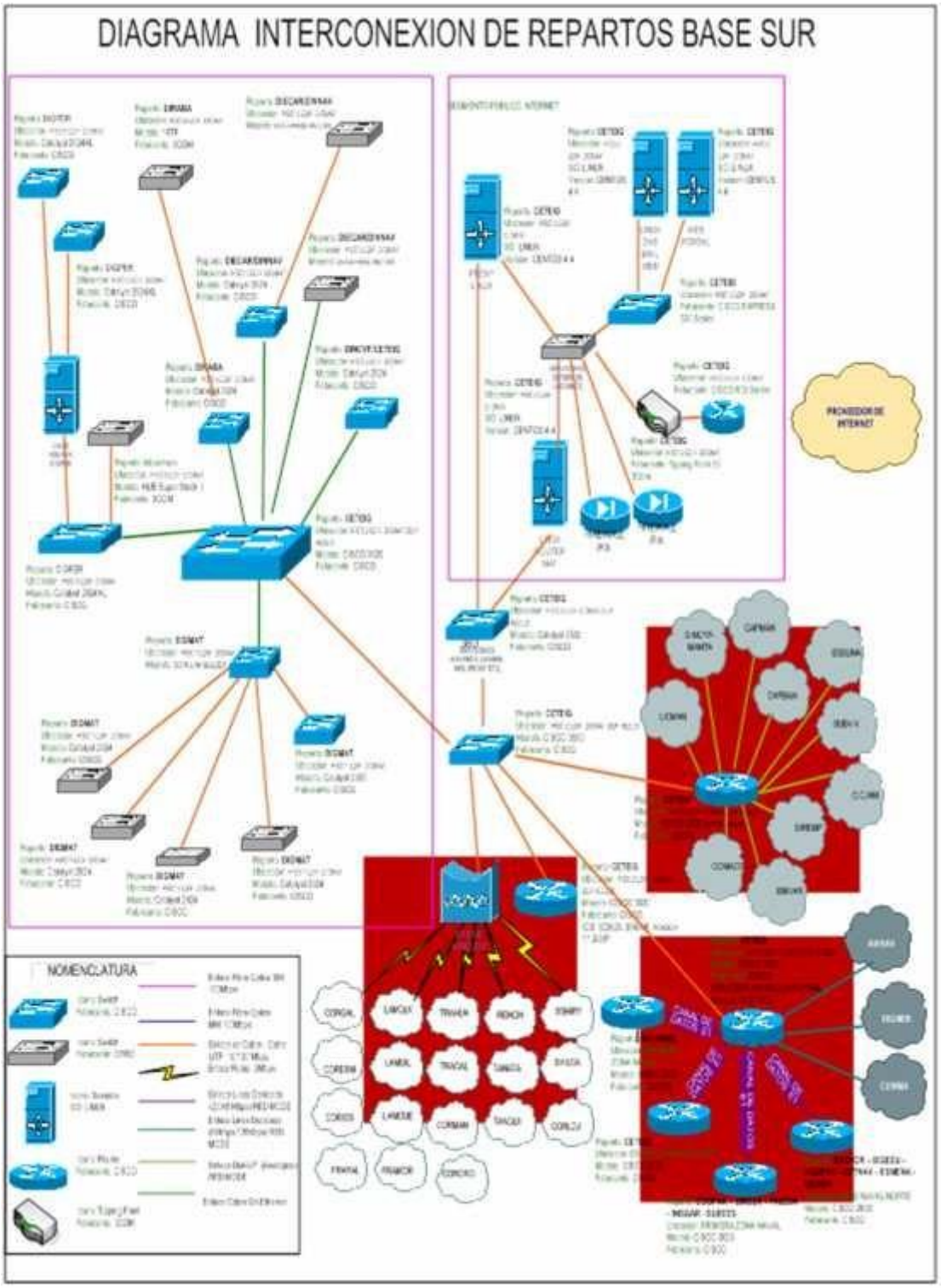
Paquete de vigilancia que se compró en la DIGMAT

Fuente: Sistema Vigilancia de la DIGMAT (CETEIN DIGMAT, 2008)
Autor: CETEIN-DIGMAT

ANÁLISIS DE LA DE RED DE LA BASE NAVAL SUR

Debido a la importancia que tienen los sistemas computarizados, el área de redes ha venido cambiando y mejorando con el paso del tiempo, es uno de los sectores en los que se ha prestado mayor atención en los últimos años.

Diagrama De Interconexión De Repartos De La Base Naval Sur

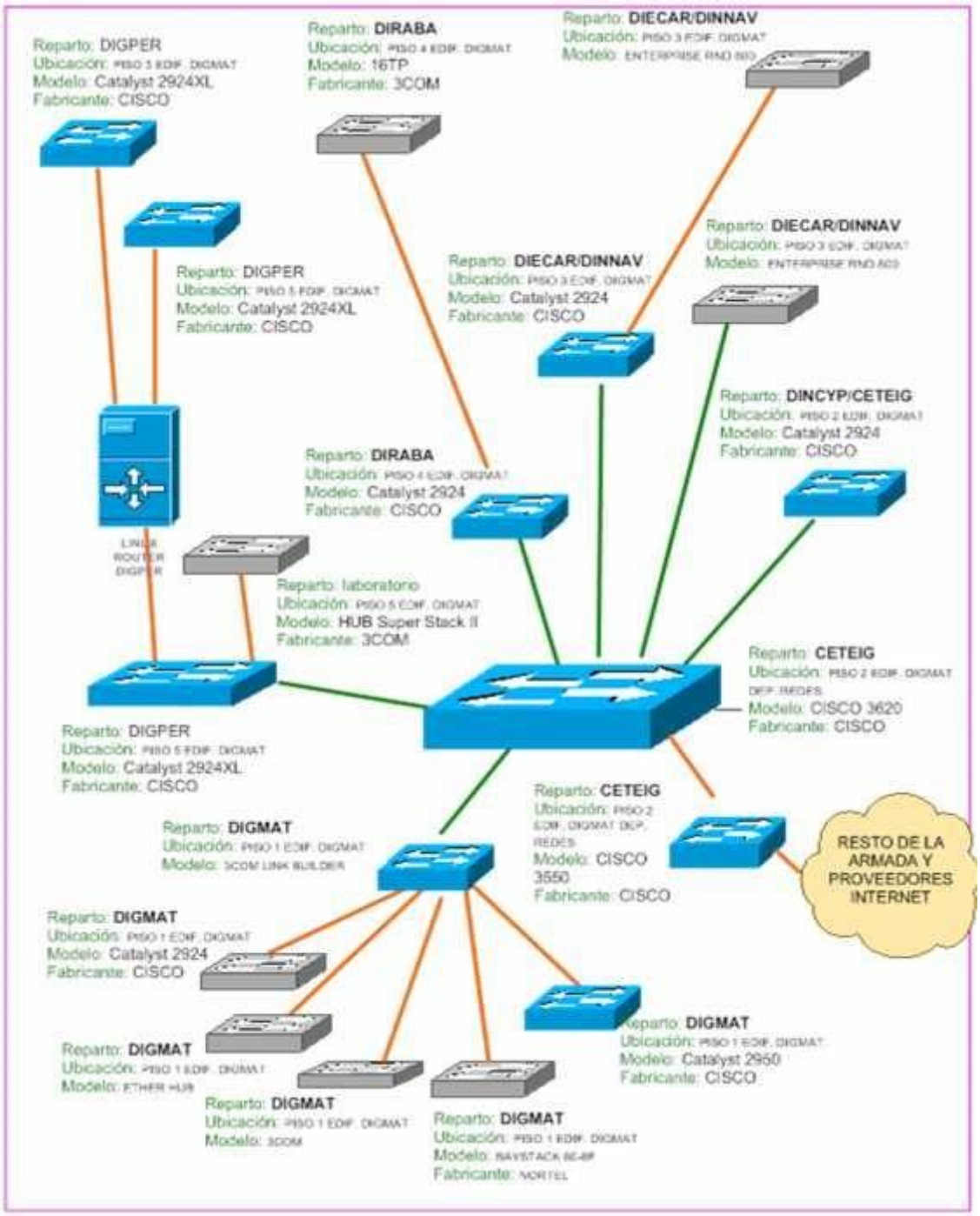


Fuente: Proporcionado por la Dirección de Tecnologías de la Información (DIRITC, 2012)

Autor: DIRTIC

DIAGRAMA DE RED DEL EDIFICIO DIGMAT

Red Edificio DIGMAT



Fuente: Proporcionado por la Dirección de Tecnologías de la Información (DIRITC, 2012)

Autor: DIRTIC

HARDWARE DE RED DE LA BASE NAVAL SUR

A continuación se muestra el detalle de los equipos que proporcionan la conectividad en la Base Naval Sur.

Equipos De Red De La Base Naval Sur

Switch Modelo.- ServerIron XL

Balanceo de Carga
(Zona Desmilitarizada Pública y Zona Desmilitarizada Privada)

Switch capa 4-7.- Distribución de servicios basados en IP con balanceo de carga transparente entre múltiples servidores, monitoreando permanentemente los servidores, las aplicaciones y el contenido. Incluye las características de Server Load Balance (SLB) y Global Server Load Balance (GSLB).

Marca.- Foundry Networks.Modelo.- ServerIron XL

Cantidad: 2Throughput: 2 Gbps

Sesiones concurrentes: 1’000.000 # IP Virtuales: Ilimitado.

Puertos 10/100: 24 # Puertos Gigabit: 2 (RJ45)

Figura 2.15
Switch Modelo.- ServerIron XL

Fuente: www.cisco.com – (CISCO)
Autor: CISCO

Switch Modelo.- Catalyst 3550-12T

Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs; alta velocidad de conmutación.

Marca.- Cisco Modelo.- Catalyst 3550-12T

Cantidad: 1 # Puertos Gigabit RJ45: 10

Puertos GBIC: 2 (RJ45)

Sistema Operativo: Enhanced Multilayer Software Image

Switch Modelo.- Catalyst 3550-12T

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

SWITCH - Modelo.- Catalyst 3550-24G

Backbone de la Red Naval de Datos

Servicios de conmutación con capacidad de soportar capa 3,

VLANs y ACLs. Marca.- Cisco

Modelo.- Catalyst 3550-24G Cantidad: 1

Throughput:1 # Puertos 10/100 RJ45: 24

Puertos GBIC: 2 (RJ45)

Sistema Operativo: Enhanced Multilayer Software Image

Servicios de conmutación con capacidad de administrar capa 3 y 4, VLANs y ACLs; Switch modular con versatilidad de interfaces y número de puertos; máquina avanzada procesadora de paquetes y agente RMON; alta velocidad de conmutación. Switch principal de la Red de Campus de la Base Naval Sur. Colapsa la red de fibra óptica monomodo de Campus, y la red de fibra óptica multimodal del edificio principal.

Backbone de la Red Naval de Datos Modelo.-
Catalyst 3550-24G

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

Firewall Marca.- Cisco Modelo.- Catalyst 4506.

Servicios de Firewall de Borde

Marca.- Cisco Modelo.- Catalyst 4506.

Procesador: Supervisor IV (2 GE) Disco Flash Memory

Modulo FX 10/100: 64 Mb Sup III/IV Módulo RJ45 10/100 + 24 puertos

GBIC: 32 puertos + 2 Módulo RJ45 Gigabit:

Otras características: Fuente de poder redundante, Sistema Operativo Cisco IOS Enhanced L3 SW C4000 SUP 3/4 (OSPF, IGRP, EIGRP), Licencia Agente RMON. 48 puertos

Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento, capacidad FailOver Activo-Pasivo. Aceleración de hardware para túneles VPN; control de tráfico entre la Zona Internet y la Zona Privada.

Firewall Marca.- Cisco Modelo.- Catalyst 4506.

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

Firewall Interno Militarizado Modelo.- PIX 515E Marca.- Cisco

Modelo.- PIX 515E (Principal y Fail Over) Marca.- Cisco

Cantidad: 1 # Zonas: 130

Marca.- Lucent TechnologiesModelo.- Brick VPN 200.

Throughput Firewall: 2 .- Throughput VPN: 6 puertos 10/100 Mbps

sesiones concurrentes: 180 Mbps

Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento. Para control de tráfico de paquetes hacia y desde la Zona Desmilitarizada Privada.

140 Mbps

Firewall Interno Militarizado Modelo.- PIX 515E Marca.- Cisco

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

Equipos De Red De La Capa De Distribución De La Red De Campus De La Base Naval Sur

SWITCH Modelo.- Catalyst 4506.

Servicios de conmutación con capacidad de administrar capa 3 y 4, VLANs y ACLs; Switch modular con versatilidad de interfaces y número de puertos; máquina avanzada procesadora de paquetes y agente RMON; alta velocidad de conmutación. Switch principal de la Red de Campus de la Base Naval Sur. Colapsa la red de fibra óptica monomodo de Campus, y la red de fibra óptica multimodal del edificio principal. Habilitación PVST.

Marca.- CiscoModelo.- Catalyst 4506 - Procesador: Supervisor IV (2 GE)

.Ubicación.- Edificio DIGMAT - CETEIG. - Módulo FX 10/100: 24 puertos

Disco Flash Memory 64 Mb Sup III/IV - GBIC: 48 puertos

Módulo RJ45 10/100 + 32 puertos + 2 - Módulo RJ45 Gigabit: ,

Sistema Operativo Cisco IOS Enhanced L3 SW C4000

Otras características: Fuente de poder redundante

SWITCH Modelo.- Catalyst 4506

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

SWITCH Marca.- Cisco Modelo.- Catalyst 3550-24-FX0

Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs. Habilitación PVST.

Marca.- Cisco.- - Modelo Catalyst 3550-24-FX

Ubicación.- Edificio CENABS - # Puertos 10/100 FX: 24

Puertos GBIC: 2 Gigabit SMF

Sistema Operativo: Enhanced Multilayer Software Image

Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs. Habilitación PVST.

SWITCH Marca.- Cisco Modelo.- Catalyst 3550-24-FX0

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

SWITCH Marca.- Cisco Modelo. Catalyst 2912-FX

Modelo.- Catalyst 2912-FX. Marca.- Cisco

Ubicación.- Edificio Talleres Integrados DIECAR

Puertos 10/100 FX: 12 # Puertos GBIC: 2 Gigabit SMF

Sistema Operativo: Enhanced Multilayer Software Image

Figura 2.22

SWITCH Marca.- Cisco Modelo. Catalyst 2912-FX

Fuente: www.cisco.com – (CISCO)

Autor: CISCO

Equipos De Red De La Capa De Acceso A La Red De Campus De La Base Naval Sur Desde El Sector Sur

SWITCH	Marca.- Cisco	Modelo.- Catalyst 2950C-24

Modelo.- Catalyst 2950C-24

Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del CENABS a la Red de Campus.

Marca.- Cisco - Cantidad.- 8

Ubicación.- Edificio CENABS - Edificio Club Naval

Edificio DIRSAN - Edificio BASUIL

Edificio HOSNAG - Edificio INOCAR

Edificio ESDESU

Edificio Gate Principal - Oficina de Seguridad

Puertos 10/100 RJ45: 24 - # Puertos 100 FX: 2

Sistema Operativo: Enhanced Multilayer Software Image

Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Escuela de Superficie a la Red de Campus.

SWITCH Marca.- Cisco Modelo.- Catalyst 2950C-24

Fuente: www.cisco.com – (CISCO)

Autor: CISCOM

ANÁLISIS DE LA SEGURIDAD

No existe un sistema que mantenga un control de los niveles de claves de acuerdo a las funciones, rangos y responsabilidades de cada usuario, Personal Naval, servidores públicos y/o Terceros.

Como se explicó anteriormente las tarjetas de acceso no son para toda la Fuerza Naval, ni para toda la Base Sur, sino que restringen el acceso a un departamento o área específica, de tal forma que se debería tener tantas tarjetas como lugares se quiera restringir el acceso.

En ocasiones el personal de "inteligencia", personal que verifica la seguridad de los Almirantes y otras personas con cargos importantes dentro de La Fuerza Naval, han burlado con tal facilidad las "Seguridades", logrando demostrar lo importante de establecer los procedimientos de seguridad en todos los niveles de La Fuerza Naval, para evitar en un futuro que ocurra realmente un atentado o algún inconveniente de graves consecuencias y lograr salvaguardar la seguridad no solo de los Almirantes sino de todo el personal que labora en la institución, los materiales e información, que hoy por hoy son activos de vital importancia en toda empresa y/o institución del mundo.

Diagnóstico del análisis de la situación actual

Diagnóstico del proceso actual

En la Fuerza Naval no se cuenta con procedimientos de seguridad físico y acceso informático que controle eficazmente el acceso a sus diferentes repartos, mucho menos se puede pensar en que se cuente con un sistema de Control de acceso automatizado y restringido. Esto es preocupante debido dentro de los recintos navales hay lugares que adquieren cierto grado de sensibilidad por el tipo y/o categoría del material que contienen, o trabajos que en él se desarrollan.

Los niveles de clave de Seguridad están ausentes, no existen accesos de control restringido, peor aún, no se cuenta con procesos de control redundante.

Si las personas ingresan en vehículo, no son registradas en ninguna parte si ingresan hasta las 08h00. debido a que es el horario de ingreso del personal. Después de esa hora se les pide la cédula pero no se registra en ninguna bitácora, ni en ningún archivo, registro, ni similiar.

De igual manera, si se desea conocer quién ingresó por las garitas de seguridad sin vehículo es el mismo proceso. En algunos casos ni anotan, solamente pasan al mostrar el carné.

Cuando ingresan a los repartos Navales propiamente dicho, en este caso al edificio de la DIGMAT, se registran en una bitácora, de tal forma que si se desea conocer si una persona ha ingresado en un periodo de tiempo en la base naval habría que revisar una a una las líneas de la bitácora al igual que en el caso de los vehículos.

Esta falta de seguridad es tan evidente que hay personas que nunca se sabe cómo ingresaron al edificio, y que van vender productos e ingresan a áreas restringidas con total normalidad.

Existe un sistema biométrico que ayuda a controlar el personal, pero solo de ciertos repartos, es decir no es obligatorio para todos, hay personas que no lo utilizan y por ejemplo los oficiales nunca marcan en el sistema biométrico.

En algunos departamentos de alto riesgo existe el control de ingreso a través de tarjeta de aproximación, este control es para el personal que labora en las áreas restringidas, pero este control para los visitantes no existe porque ingresan cuando se abre la puerta, pero no se registra en ningún lado el ingreso de estas personas. Hay departamentos que deben tener mayor restricción porque se almacenan datos de vital importancia para la institución y que no poseen ningún tipo de seguridad especial.

Todos los sistemas antes mencionados están conectados a base de datos independientes cada una por su lado y no existe una vinculación entre los diferentes sistemas de control de ingreso.

En cuanto a los sistemas informáticos, cada vez que un usuario cambia de funciones se le asigna nuevamente los permisos al sistema informático. Con nuevo usuario y clave, muchas veces demora demasiado tiempo en que se le otorguen los permisos respectivos.

Diagnóstico de la red del edificio digmat

La distribución de redes es inadecuada puesto que deja sectores en la intranet sin controles estrictos de seguridad poniendo en peligro la infraestructura completa de la Institución.

El principal problema que tienen las redes es que no cuentan con un Firewall en los enlaces con los otros repartos de La Fuerza Naval, ya que estos repartos, tienen a su vez conexiones con proveedores, un sinnúmero de amenazas que ponen en peligro la red de la Base Naval Sur.

Este inconveniente se debe a que las Fuerzas Navales se han preocupado por cubrir el acceso desde el exterior, olvidándose que los accesos de la intranet pueden ser tanto o más peligrosos.

Existen repartos que manejan individualmente sus accesos a internet, es decir contratan los servicios a terceros y no accedan a los sistemas centrales, por lo tanto, ellos necesitarían firewalls especiales, esto hace vulnerable a la DIGMAT.

Diagnóstico del hardware

El Hardware de la Base sur en lo que es seguridad es muy básico, se necesitan servidores para la base de datos que soporte el flujo de información que involucra la seguridad de la base.

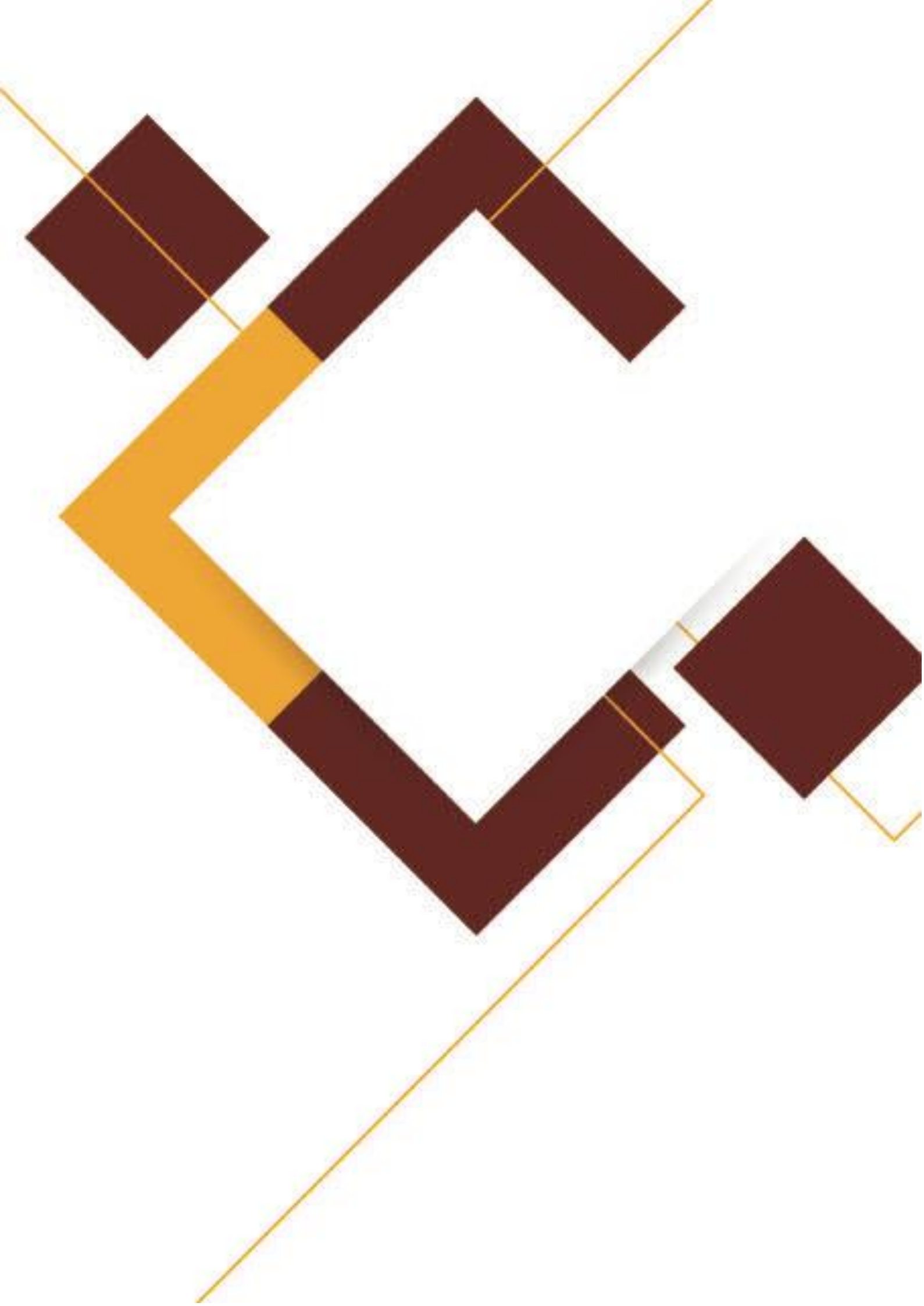
En cuento a cámaras, no existen en lugares de acceso de ingreso, ni en los caminos especialmente los que conducen a las áreas restringidas. Apenas se cuenta con las cámaras en el edificio DIGMAT-DIGREH.

Al personal que debe monitorear estas cámaras se les asigna otras funciones adicionales. No se guardan los archivos de las grabaciones en un servidor, ni en DVD con el fin de evitar costos.

Algunas de las cámaras se han averiado y no han sido reparadas. No existe personal capacitado en el manejo integral el sistema de seguridad

Diagnóstico de sistema biométrico de la digmat

El sistema Biométrico, como los otros pequeños sistemas utilizados en la DIGMAT y sus repartos subordinados, solo sirven para llevar el control de la asistencia de los empleados, los mismos que deben ser registrados en cada uno de los sistemas tanto Biométricos como de tarjetas de aproximación. Es decir que en cada reparto, departamento o sección existe una base de datos independiente, es por este motivo que se deben unificar en un solo sistema de registro de ingreso de personal; pero además, este sistema debe contemplar el ingreso de visitas tanto de otros repartos, departamentos o secciones como de proveedores y visitantes en general.



CAPITULO 3

Planificación estratégica

Este Capítulo se destinará a la evaluación de los factores internos y externos que afectan a la eficiencia de la Fuerza Naval del Ecuador y específicamente a la situación planteada en el presente proyecto: emitir estrategias y tácticas para lograr los objetivos y metas planteadas.

MATRIZ DE EVALUACIÓN DE FACTORES INTERNOS (MEFI)

> *Para determinar el valor ponderado se utilizó la siguiente tabla de valores y clasificación para determinar el valor ponderado de las fortalezas y debilidades Se asigno un peso entre 0.0 (no importante) a 1.0 (absolutamente importante) a cada uno de los factores. El peso adjudicado a un factor dado indica la importancia relativa del mismo para alcanzar el éxito en la industria de la empresa. Independientemente de que el factor clave represente una fuerza o una debilidad interna, los factores que se considere que repercutirán más en el desempeño de la organización deben llevar los pesos más altos. El total de todos los pesos debe sumar 1.0*
>
> *Se asignó una calificación entre 1 y 4 a cada uno de los factores a efecto de indicar si el factor representa una debilidad mayor (calificación =1), una debilidad menor (calificación =2), una fuerza menor (calificación =3) o una fuerza mayor (calificación =4). Así, las calificaciones se refieren a la compañía, mientras que los pesos del paso 2 se refieren a la industria*. (CERTO, y otros, 1997)

Parámetros para la ponderación de los Factores Internos

	Valor	*El valor asignado a determinado factor indica la importancia relativa del factor para que sea exitoso en la industria de la empresa. La sumatoria de los valores debe ser igual a 1*
0,0	*Sin importancia*	
1,0	*Muy importante*	
	Clasificación del factor externo clave	
4	*Excelente*	
3	*Arriba del promedio*	
2	*Nivel promedio*	
1	*Deficiente*	
	Valor Ponderado	
4	*Más alto posible*	
3	*La empresa mantiene una posición sólida*	
2,5	*Promedio*	
1	*Más bajo posible*	
	Caracteriza a las empresas que son débiles internamente	

Fuente: Mejoramiento de los Procesos de la Empresa (CERTO, y otros, 1997)

Autor: Ing. Cecibel León Arreaga

ANÁLISIS MATRIZ DE EVALUACIÓN DE FACTORES INTERNOS (MEFI)

Los resultados ponderados de la Matriz MEFI está por debajo de 2.5, con un valor exacto de 2.25 lo que indica que la organización presenta una situación interna un tanto desfavorable donde predominan las debilidades frente a las fortalezas. Se concluye que Fuerza Naval del Ecuador debe seguir estrategias que tiendan a la aplicación y mejora continua de procesos y procedimientos de seguridad.

Matriz de Evaluación de Factores Internos

FACTORES INTERNOS CLAVES				
	FORTALEZAS	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
1.-	F1. La Institución cuenta con recursos Financieros	0,1	4	0,4
2.-	F2. La disciplina militar es muy buena y ayudaría a la implementación.	0,1	3	0,3
3.-	F3. Equipo humano joven y con sólidos conocimientos que ayudan hacia la mejora avanzado sistema de gestión y optimización de recursos.	0,1	3	0,3
4.-	F4. Poder unirse a otros proyectos de Seguridad para poder adquirir ciertos equipos.	0,1	4	0,4
	DEBILIDADES	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
1.-	D1. No se planifica adecuadamente el presupuesto de Seguridad	0,1	1	0,1
2.-	D2. Existen instalaciones que prestan servicios al publico en general tales Banco de Rumiñahui y el Club Naval, junto a áreas restringidas.	0,1	2	0,2
3.-	D3. Los Militares de alto rango cuando necesitan se saltan los procedimientos de seguridad	0,05	2	0,1
4.-	D4. Inexistencia de procedimiento bien establecidos para el manejo de Seguridad en la Base Naval	0,1	1	0,1
5.-	D5. No se cuenta con los equipos de seguridad necesarios	0,05	1	0,05
6.-	D6. No se cuenta con firewall para los enlaces internos de la Armada.	0,1	2	0,2
7.-	D7. La cadena de mando hace engorroso cualquier cambio que se desee aplicar	0,1	1	0,1
	TOTAL	1		2,25

Fuente: Mejoramiento de los Procesos de la Empresa (CERTO, y otros, 1997)

Autor: Ing. Cecibel León Arreaga

MATRIZ DE EVALUACIÓN DE FACTORES EXTERNOS (MEFE)

En primer lugar se realizó una lista de los factores de éxito; primero las oportunidades y después las amenazas.

> *Se asignó un peso entre 0.0 (no importante) a 1.0 (absolutamente importante) a cada uno de los factores. El peso indica la importancia que tiene ese factor para alcanzar el éxito en la industria de la empresa.*

Se asignó una calificación entre 1 y 4 a cada uno de los factores a efecto de indicar si el factor representa, donde 4= una respuesta superior, 3= una respuesta superior a la media, 2= una respuesta media y 1= una respuesta mala. Las calificaciones se basan en la eficacia de las estrategias de la empresa. Así, las calificaciones se refieren a la compañía.

Se Multiplicó el peso de cada factor por su calificación correspondiente para determinar una calificación ponderada para cada variable. La Suma las calificaciones ponderadas de cada variable para determinar el total ponderado de la organización entera. Sea cual fuere la cantidad de factores que se incluyen en una matriz MEFE, el total ponderado pude ir de un mínimo de 1.0 a un máximo de 4.0, siendo la calificación promedio de 2.5. Un promedio ponderado de 4.0 indica que la organización está respondiendo de manera excelente a las oportunidades y amenazas existentes en su industria (CERTO, y otros, 1997)

Parámetros para la ponderación de los Factores Internos

	Valor
0,0	Sin importancia
1,0	Muy importante
	Clasificación del factor externo clave
4	Excelente
3	Arriba del promedio
2	Nivel promedio
1	Deficiente
	Valor Ponderado
4	Más alto posible La empresa responde de manera sorprendente a las oportunidades y amenazas presentes en el sector Las estrategias de la empresa aprovechan en forma eficaz las oportunidades existentes y reduce al mínimo los factores potenciales de las amenazas externas.
2,5	Promedio
1	Más bajo posible La estrategia de la empresa no aprovecha las oportunidades ni evita las amenazas.

Fuente: Mejoramiento de los Procesos de la Empresa (CERTO, y otros, 1997)

Autor: Ing. Cecibel León Arreaga

ANÁLISIS DE LA MATRIZ DE EVALUACIÓN DE FACTORES EXTERNOS (MEFE)

Los resultados ponderados de la Matriz MEFE está por encima de 2.5, con un valor exacto de 2.55, lo que indica que la organización presenta una situación externa prometedora para realizar un proyecto de seguridad puesto que indica que las amenazas de la Fuerza Naval pueden ser minimizadas con las oportunidades y, que lo que hay que mejorar son las estrategias externas para la aplicación y mejora continua de procesos y procedimientos de seguridad.

Matriz de Evaluación de Factores Externos

FACTORES EXTERNOS CLAVES				
	OPORTUNIDADES	*VALOR*	CLASIFI-CACIÓN	VALOR PONDERADO
1.-	O1. El Ministerio de Defensa apoya los planes de Seguridad a través de una Directiva	0,15	4	0,6
2.-	O2. Existe interés en el alto mando de la Fuerza Naval por un proyecto integral de seguridad	0,15	3	0,45
3.-	O3. Proyectos de intercambio comercial con el exterior e interior del país por ayudan a abaratar los costos	0,15	3	0,45
4.-	O4. El Gobierno este solicitando el cambio de los sistemas informáticos, para que sean hechos con software open source lo que podemos aprovechar para realizar un sistema de seguridad	0,15	3	0,45
	AMENAZAS	*VALOR*	CLASIFI-CACIÓN	VALOR PONDERADO
1.-	A1. El proceso de Financiamiento es lento y engorroso debido a la Dependencia Financiera total del estado	0,1	2	0,2
2.-	A2. Resistencia de Alto Mando al Cambio informático	0,1	1	0,1
3.-	A3. Otros repartos que planifican gastos, toman el dinero de las partidas de seguridad para organizar su proyecto	0,1	2	0,2
4.-	A4. Exposición a un posible ataque subversivo	0,1	1	0,1
	TOTAL	*1*		*2,55*

Fuente: Mejoramiento de los Procesos de la Empresa (CERTO, y otros, 1997)

Autor: Ing. Cecibel León Arreaga

MATRIZ DE LAS FUERZAS–OPORTUNIDADES – DEBILIDADES – AMENAZAS (FODA)

"FODA" es una metodología de estudio de la situación competitiva de una empresa en su mercado (situación externa) y de las características internas (situación interna) de la misma, a efectos de determinar sus ***D****ebilidades,* ***O****portunidades,* ***F****ortalezas y* ***A****menazas.*

La situación interna se compone de dos factores controlables: fortalezas y debilidades, mientras que la situación externa se compone de dos factores no controlables: oportunidades y amenazas.

Es la herramienta estratégica por excelencia más utilizada para conocer la situación real en que se encuentra la organización.

En nuestro caso para realizar la Matriz FODA previamente hemos realizado el análisis de los Factores Internos y el análisis de los factores externos, con estos datos vamos a realizar la Matriz FODA cuyo núcleo consiste en determinar cuáles serían las estrategias más relevantes a seguir para lograr el objetivo de la empresa y en nuestro caso el objetivo planteado en el proyecto. (Fred, 1997)

Ver Figura 3.5

Descripción de estrategias y tácticas

El objetivo principal de la planeación estratégica es llegar a determinar cuáles son las estrategias que lograran mejorar el desempeño y competitividad de una empresa o institución.

> **Estrategias**. En este ítem se responde a la pregunta *¿cómo hacerlo?* Las estrategias existen asociadas a objetivos y muestran cómo la empresa va a utilizar sus recursos para alcanzar sus objetivos. Si el objetivo es aumentar el 10% las ventas del producto x, la estrategia puede ser ampliar el y % la cantidad de (Ambrosio, 1978)

1. Estrategia de automatización: marcar una diferenciación logrando automatizar los procesos de seguridad a traves de sistemas de comunicaciones e informáticos.

   Es importante marcar una diferenciación automatizando los procesos de seguridad. Los países que rodean al Ecuador, presentan sus propios problemas de atentados y problemas políticos, lo que deja entrever la necesidad de mantener sistemas de seguridad más seguros.

   Además con un sistema automatizado los altos mandos podrán obtener de forma inmediata toda la información necesaria para poder realizar una toma de decisiones

   Para que el plan sea confiable, deben desarrollarse tácticas realistas y de acuerdo con los plazos previstos, (Ambrosio, 1978) eso significa que aunque tengamos un plan estratégico bien desarrollado si no lo aterrizamos a la realidad del mercado o de la empresa no nos va a servir de mucho.

   Tácticas

   1.1. Presentar un proyecto de Seguridad Integral automatizada al alto mando.

   1.2. Conseguir los recursos necesarios para poner en marcha el proyecto.

   1.3. Realizar el programa de adquisición para que sea aprobado por el gobierno

1.4. Contratar al personal y/o empresa que implemente el sistema informático de seguridad.

1.5. Realizar un programa de promoción del sistema para darlo a conocer a todos los miembros de la Fuerza Naval y capacitarlos en el manejo del mismo.

2. Estrategia de financiamiento: aprovechar la disponibilidad de recursos para motivar la inversión por parte del gobierno central y alto mando militar en asuntos de seguridad de la fuerza naval.

   Es evidente que el gobierno Ecuatoriano está muy interesado en la seguridad de las instalaciones de la Fuerza Naval e instituciones públicas, por lo que sería importante aprovechar esta predisposición por parte del gobierno y motivarlos para que inviertan en la seguridad de la Fuerza Naval

   Tácticas

   2.1. Presentar un proyecto de Seguridad Integral automatizada al alto mando.

   2.2. Realizar un estudio de las diferencias con las Armadas de Sudamérica y Latinoamérica y la del Ecuador para demostrar la necesidad de mejorar el sistema de seguridad.

   2.3. Demostrar con estudios respecto de un posible atentado para demostrar la necesidad de la mejora de la seguridad Institucional, esto puede hacerse con ayuda de la Dirección de Inteligencia Institucional.

3. Estrategia de publicidad y motivación: concientizar al alto y medio mando sobre la necesidad de elaborar planes de seguridad actualizados.

   En la Actualidad se emiten disposiciones de realizar un plan de seguridad cada año en la Institución pero, nunca se realiza una verdadera planificación,

en lo único que se piensa es en la captación de recursos, por ende, estas supuestas planificaciones no responden a las necesidades de la Institución.

Tácticas

3.1. Emitir un proyecto global de seguridad por parte del Alto mando.

3.2. Realizar un programa de capacitación y promoción del Plan de Seguridad Institucional, y de la necesidad del mismo al mando medio para concientizarlo sobre el seguimiento de los procesos y procedimientos de seguridad.

3.3. Realizar programas de simulacros de infiltraciones cuyos resultados sean expuestos al medio mando para que ellos sientan el peso de su responsabilidad para que no se den infiltraciones reales.

4. Estrategia de gestion: elaborar un sistema de gestión para la planificación, seguimiento y control de las políticas, procesos y procedimientos de seguridad

Tácticas

4.1. Planificar la elaboración de procesos de seguridad que respondan a las necesidades de cada uno de los repartos de la Fuerza Naval.

4.2. Destinar un grupo de colaboradores de la Fuerza Naval, con ayuda de la Dirección de Recursos humanos para hacer un grupo de trabajo altamente capacitado que ayude a la elaboración de los procesos y procedimientos de seguridad.

4.3. En base a los datos obtenidos en los puntos 4.1 y 4.3 elaborar la política de seguridad, objetivos, valores, etc.

4.4. Implementar normativas de seguridad Institucional

4.5. Realizar inspecciones que sirvan de retroalimentación para ver el cumplimiento de las normativas.

4.6. Realizar correctivos con los datos obtenidos de las inspecciones.

4.7. Capacitar a los miembros de la institución para corregir los errores o faltas encontrados.

4.8. Llevar estadísticas reales de los incidentes y accidentes de seguridad.

5. ESTRATEGIA DE PERSONAL: CONTRATAR EL PERSONAL CAPACITADO Y/O OUTSOURCING QUE AYUDE A LA INSTALACIÓN DE LOS EQUIPOS DE SEGURIDAD NECESARIOS

Tácticas

5.1. Determinar los responsables del proyecto por áreas.

5.2. Contratar personal con altos conocimientos en equipos de seguridad y telecomunicaciones.

5.3. Contratar o aprovechar el personal de la empresa para el desarrollo del sistema informático.

VISIÓN

Lograr que la Fuerza Naval del Ecuador tenga un alto grado de modernización y se encuentre altamente capacitada en Seguridad interna.

MISIÓN

Planificar, organizar, capacitar, equipar y mantener un alto grado de desarrollo de la seguridad, con la finalidad de contribuir a que se cumplan las políticas, objetivos y metas de la Fuerza Naval.

OBJETIVOS

Primero se analiza una descripción de lo que son los objetivos a largo plazo:

> **Los objetivos a largo plazo:** Son los resultados específicos que pretende alcanzar una organización por medio del cumplimiento de su misión básica. Largo plazo significa más de un año. Los objetivos son esenciales para el éxito de la organización por que establecen un curso, ayudan a la evolución, producen sinergia, revelan prioridades, permiten la coordinación y sientan

> las bases para planificar, organizar, motivar y controlar con eficacia. Los objetivos deben ser desafiantes, mensurables, consistentes, razonables y claros. (Fred, 1997; Fred, 1997)

Implementar un Sistema de Seguridad 100% automatizado, a la vanguardia en el Ecuador que permita el control del acceso a las diferentes áreas del edificio de la Dirección General del Material en un plazo máximo de 1 año.

Lograr que el personal este 100% capacitado sobre el reglamento de seguridad de la institución en un plazo de 2 años como máximo.

METAS

> Una vez definidos los objetivos y escogidas las estrategias, es necesario definir una programación de ejecución para estipular qué resultados deben ser alcanzados, cuándo deben ser conseguidos y *por quién* deben ser logrados. Por ejemplo, el departamento de ventas deberá aumentar las ventas del producto *x* el 2% en el primer trimestre, el 4% en el segundo, el 3% en el tercero y el 1% en el cuarto trimestre. (Ambrosio, 1978)

Dotar en un 100%, al edificio, de cámaras de seguridad en lugares estratégicos en el plazo de 1 año, con el objetivo de mantener un control de las personas que ingresan al edificio y en que pisos circulan.

Instalar en el plazo de 1 año lectores de tarjetas de proximidad en el 100% de las puertas de a las áreas que se considere necesario, en los diferentes pisos del Edificio DIGMAT, de acuerdo a un estudio previo, para mejorar el control del ingreso y salida de las personas a los diferentes departamentos en la institución.

Dotar en 1 año de Controles biométrico en las áreas que tienen mayor grado de sensibilidad, es decir que deben tener mayor resguardo, por lo menos en un 70%.

Implementar, en 6 meses, una base de datos que se conecte a los diferentes controles instalados, integrándolos automáticamente.

Implementar un software que ayude al control del personal que labora en el edificio, y a los visitantes. Guardando un histórico de los datos, en un plazo máximo de 6 meses.

Contar en 1 año, con una estación de control que permita dar los permisos respectivos a cada usuario y que a su vez sirva para el control visual de las cámaras de seguridad.

Capacitar gradualmente, en un 25% anual hasta llegar al 100%, al personal para que pueda utilizar adecuadamente el software que se va a instalar y sobre los reglamentos de seguridad internos.

MATRIZ DEL PERFIL COMPETITIVO (MPC)

Los datos y conceptos fueron obtenidos del libro Conceptos de administración estratégica. (Fred, 1997)

La matriz de perfil competitivo identifica a los principales competidores de la institución, así como sus fuerzas y debilidades particulares, en relación con una muestra de la posición estratégica de la empresa. Los factores de una MPC incluyen cuestiones internas y externas; las calificaciones se refieren a las fuerzas y debilidades. Los factores críticos o determinantes para el éxito en una MPC son más amplios, no incluyen datos específicos o concretos, e incluso se pueden concentrar en cuestiones internas.

Los competidores seleccionados fueron: la Armada de Perú y la Armada de Chile, basándose en los siguientes factores críticos:

- Imagen internacional
- Imagen ante el pueblo
- Preparación Física
- Preparación Estratégica
- Disciplina Militar
- Nivel de automatización de los Procesos
- Tecnología informática

Se asignó un peso desde 0.0 (no importante) a 1.0 (absolutamente importante) a cada uno de los factores. El peso indica la importancia que tiene ese factor para alcanzar el éxito en la industria de la empresa. Las oportunidades suelen tener los pesos más altos que las amenazas, pero estas, a su vez, pueden tener pesos altos si son especialmente graves o amenazadoras. Los pesos adecuados se pueden determinar comparando a los competidores que tienen éxito con los que no lo tienen o analizando el factor en grupo y

llegando a un consenso. La suma de todos los pesos asignados a los factores debe sumar 1.0.

Se asignó una calificación entre 1 y 4 a cada uno de los factores a efecto de indicar si el factor representa, donde 4= mayor fuerza, 3= menor fuerza, 2= menor debilidad y 1= mayor debilidad. Las calificaciones se basan en la eficacia de las estrategias de la empresa.

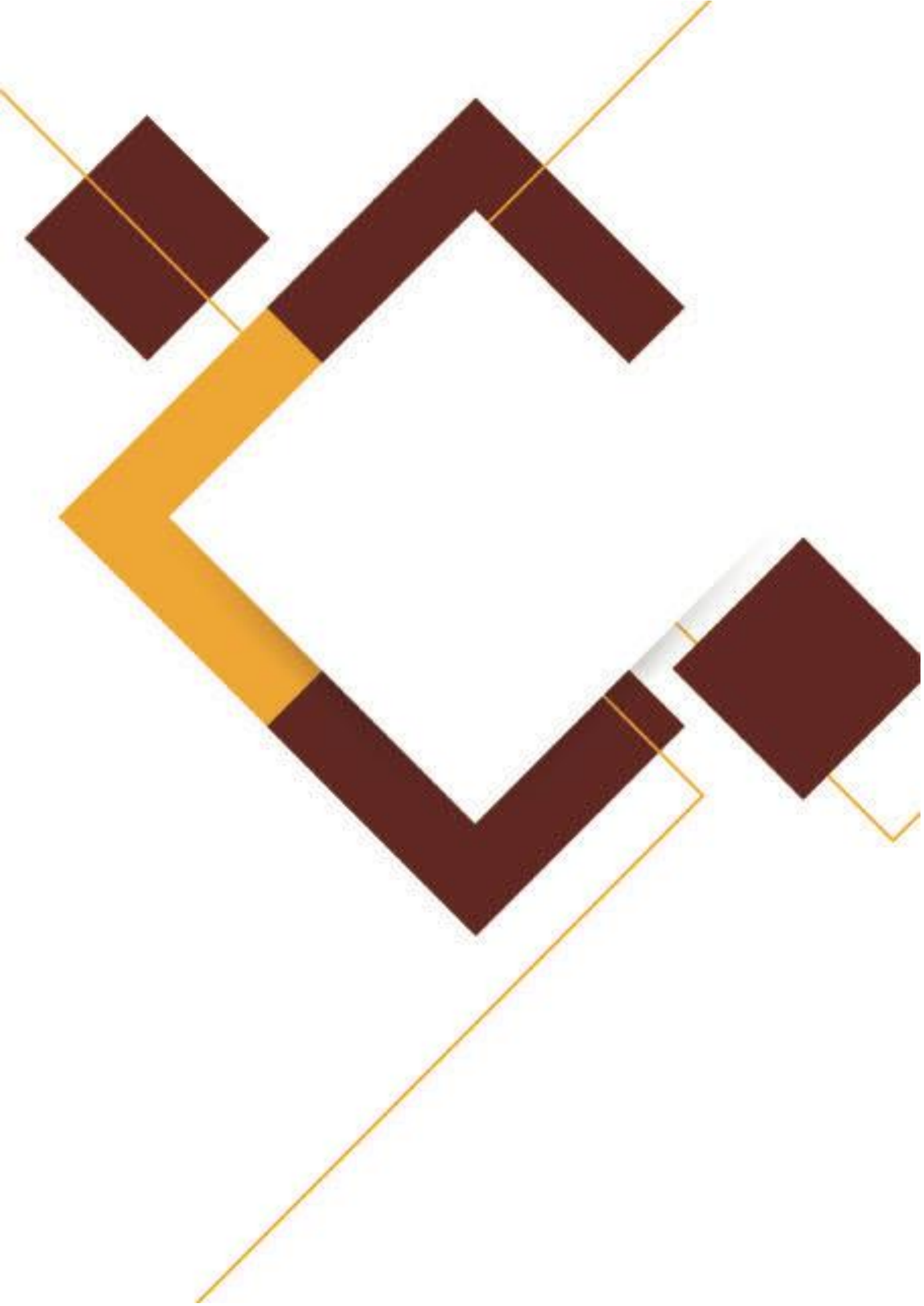
De los totales ponderados se determinó la posición en que se encuentra nuestra empresa con respecto a sus competidores.

INTERPRETACIÓN DE LA MATRIZ DEL PERFIL COMPETITIVO (MPC)

Vemos que, de los países seleccionados para realizar la matriz de perfil competitivo, el de mayor fortalezas es Chile, que se encuentra en mayor grado de automatización, teniendo ya 15 años automatizando sus procesos de manera integral, **con ayuda de un sistema llamado salino.** Su imagen ante el pueblo es buena puesto que confían mucho en su marina. La automatización de sus procesos le ha llevado a tener mayor control en los aspectos de disciplina, imagen, preparación física y estratégica.

Perú tiene ventajas sobre Ecuador en las Fortalezas de Nivel de automatización de procesos y en preparación física.

Como se ve, **a Ecuador le urge ingresar a automatizar sus procesos en general** para mejorar la *performance* de sus acciones y sobre todo de la toma de decisiones.



CAPITULO 4

Implementación del sistema y niveles de seguridad propuesto

Con el fin de explicar de manera clara el proyecto, se dividirá los niveles de seguridad en Seguridad Informática y Seguridad Física

Seguridad Informática

Se propone implementar un sistema informático que mantenga un control de los niveles de claves de acuerdo a las funciones, rangos y responsabilidades de cada usuario, Personal Naval, servidores públicos y/o Terceros, al hablar de sistema informático nos referimos a todo lo que un sistema involucra no solo al software, sino las políticas de seguridad, las auditorías, los procedimientos.

Procedimientos que se debe considerar para la seguridad informática:

- Otorgar (retirar) el acceso de personas a las tecnologías de información y como se controla el mismo.
- Asignar (retirar) derechos y permisos sobre los ficheros y datos a los usuarios.
- Autorizar (denegar) servicios a los usuarios. Tales como: Correo Electrónico, Internet)
- Definir perfiles de trabajo.

Autorización y control de la entrada/salida de las tecnologías de información.

Gestionar las claves de acceso considerando para cada nivel el tipo de clave atendiendo a su longitud y composición, la frecuencia de actualización, quién debe cambiarla, su custodia, etc.

Realización de salva de respaldo, según el régimen de trabajo de las áreas, de forma que las salvas se mantengan actualizadas, y las acciones que se adoptan para establecer la salvaguarda de las mismas, de forma que se garantice la compartimentación de la información según su nivel de confidencialidad.

Garantizar que los mantenimientos de los equipos, soportes y datos, se realicen en presencia y bajo la supervisión de personal responsable y que en caso del traslado del equipo fuera de la entidad la información clasificada o limitada sea borrada físicamente o protegida su divulgación.

Salva y análisis de registros o trazas de auditoría, especificando quien lo realiza y con qué frecuencia.

Resumen de los permisos al área Física a través de los sistemas y sistemas informáticos propiamente dicho

PERFIL DE USUARIOS	ÁREAS			SISTEMA INFORMÁTICO				
	Públicas	De Trabajo	Restringidas	Canales Públicos	Temas de Consulta	Ingreso, Modificación, eliminación	Reportes estadísticos departamentales	y Reportes
Visitante	X			X				
Tripulantes de Reparto	X	X		X	X	X		
Oficiales de Reparto	X	X	X	X	X	X	X	
Comandantes de Reparto	X	X	X	X	X	X		X

Se debe aclarar casos especiales y específicos:

1. Un visitante podrá acceder a áreas de Trabajo y/o áreas restringidas con la solicitud escrita firmada por un miembro de la fuerza que se hace responsable de los actos y seguridad del visitante en cuestión

2. Un Oficial o tripulante es considerado visitante cuando se encuentre fuera de su área de trabajo. Es decir que si va a un reparto y/o departamento donde no cumpla funciones se lo considera visitante en esa área.

3. Los perfiles de cada sistema están definido de acuerdo a las funciones específicas de cada miembro y son dictadas por perfiles especiales que tiene cada sistema. Por ejemplo en el sistema de recursos humanos existe el perfil público, el perfil de usuario Operador y el Usuario Administrador.

Seguridad Física

Para comenzar, se debe definir en qué consiste la **Seguridad Física** en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"(1). Se refiere a los controles y mecanismos de seguridad dentro y alrededor de la empresa.

Tipos de Desastres

Como se sabe, cada sistema es único es por ello que al definir la política de seguridad a implementar esta será única. Se debe aplicar siempre se pautas de aplicación general y no procedimientos específicos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra la Fuerza Naval.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Los peligros más importantes que ocurren en cualquier instalación son:

1. Incendios
2. Inundaciones
3. Condiciones Climatológicas
4. Instalaciones Eléctricas
5. Robo
6. Sabotaje

Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

4. Utilización de Guardias
5. Utilización de Detectores de Metales
6. Utilización de Sistemas Biométricos
7. Verificación Automática de Firmas (VAF)
8. Seguridad con Animales
9. Protección Electrónica

Fuente: http://www.segu-info.com.ar/fisica/seguridadfisica.htm

Propuesta de seguridad física

La propuesta de seguridad física se divide en los siguientes módulos.
Circuito cerrado de televisión.
Control de Accesos.
Alarmas contra robo, incendio, asalto.
Central de Monitoreo de Toda la información.
Sistema de detección perimétrica.
Sistemas de protección de zonas de riesgo.

Circuito Cerrado de Televisión.

Estará constituido por un circuito de cámaras de televisión que sirvan para controlar las calles de de acceso y tránsito, entradas, salidas, el estero.

Las cámaras de televisión tendrán la capacidad de transmitir la señal de video a color y serán cámaras con movimiento de giro vertical y horizontal, con lente que permita un acercamiento de mínimo 26 veces el tamaño original. Estas cámaras cubrirán todos los sectores de la base sur de tal forma que, no quede un solo paso sin la capacidad de ser divisado. Estas cámaras móviles deben tener la protección necesaria para evitar los sabotajes y vandalismos. A este tipo de cámaras se los conoce como **Autodomos,**

servirán para el día y la noche, en el día a colores y en la noche a blanco y negro con infrarrojos.

A través de la fibra óptica la señal de las cámaras será enviada a servidores de video, desde donde esta información podrá ser utilizada por los sistemas informáticos de seguridad propios de la base. (Sistema de Seguridad a Desarrollar).

La señal de video será grabada en video digital en un sistema que tiene la capacidad para soportar 30 días de grabación ininterrumpidos sin necesidad de sacar respaldo, aunque por seguridad y haciendo una redundancia de seguridad se deberá hacer un espejo de este servidor, el respaldo puede ser además sacado a través de un DVD writer. Se puede grabar simultáneamente de todas las cámaras.

La señal de las cámaras podrá ser visualizada a través de monitores de 42" en un cuarto de control que estará ubicado en la planta baja de DIGMAT, el sistema permite hacer zoom y a su vez dividir la pantalla en 4 partes. Y permite así el control de 4 cámaras a la vez, los equipos que conforman el sistema son:

a. 20 Autodomos PTZs de 1/3 a color con Zoom de un mínimo de 26 X, blindajes y monturas para ser instalados en el exterior.
b. 12 cámaras a color con lente varifocal, autoiris, blindaje y montura para cubrir entrada y salida en la garita principal y el área operativa.
c. 02 Sistema de video grabación digital con disco duro de 1 terabyte y multiplexor de 16 canales de entrada.
d. 19 Sistema de video transmisión a través de fibra óptica.

<u>Ubicación de los Autodomos</u>

1. Dique flotante
2. Dique flotante sector guardacostas
3. Área operativa hacia ASTINAVE
4. Área operativa hacia muelle de submarinos
5. Garita del área operativa
6. Sector de transportes y gasolinera.
7. Esquina de la calle BASUIL 3 control a portuaria.
8. Ingreso ASTINAVE por bloques de tripulantes.

9. Club naval.
10. Calle DIRSAN, BASUIL, HOSNAV.
11. Calle escuela de superficie comisariato.
12. Bloque de tripulantes control 25 de julio.
13. Garita de entrada principal.
14. Entrada 25 de julio a COGUAR.
15. Esquina de edificio DIGMAT y área de DIRBIE.
16. Esquina de bloque de oficiales hacia estero.
17. Esquina de bloque de oficiales hacia calle COGUAR.
18. Club naval, control estero caracol.
19. Garita COGUAR.
20. Por definir.

Presupuesto 36.150 dólares Americanos Incluida instalación y puesta en marcha y cableado.

Sistema de control de acceso

Este sistema permitirá controlar y restringir la entrada de personal y de vehículos a las distintas zonas de BASUIL (Base Naval Sur).

Las áreas a restringir el acceso pueden ser consideradas de los siguientes tipos:

Acceso a una puerta cerrada por una chapa electromagnética o eléctrica.

Acceso en una garita de entrada controlada con un sistema informático, que ayudará al control del personal que labora en las instalaciones de BASUIL como a las personas que visitan las mismas.

Acceso a una calle de ingreso de una aérea restringida por medio de una barrera eléctrica

Todos estos elementos serán accionados con una lectora de tecnologia a escoger, puede ser proximidad, Biométrica, etc. que permitirá o no el acceso de la persona o vehículo, al área restringida.

Todos los vehículos de las bases navales podrán tener un dispositivo de lectura de

radio frecuencia que permita controlar y leer directamente la información, así como conceder o no el paso a esa arrea a un vehículo.

Los torniquetes, chapas electromagnéticas. Puertas y vallas eléctricas de seguridad, podrán ser operadas en forma automática a través de tarjetas de proximidad que tendrán los usuarios permanentes de recinto o en forma manual por el personal de guardia que levantara la valla o abrirá una puerta, etc. una vez autorizado el ingreso.

Estas tarjetas universales podrán servir también como identificación naval y único documento que le permita el ingreso.

El sistema de control de accesos estará en capacidad de: Permitir el ingreso de la persona o vehículos que presenta la tarjeta en la lectora.

Sacar todo tipo de reportes de una o varias tarjetas, en cierto horario, fecha, o lugar de asignación.

Este sistema estará en la capacidad de trabajar en conjunto con el sistema de LA RED DE DATOS creada en cada reparto, registrar la persona que entró y salió con la información de horario y fecha. Este sistema tendrá la capacidad de imprimir los reportes necesarios de la información que sea requerida.

Este sistema en un inicio estará destinado para controlar el ingreso en la entrada principal y el área operativa.

> Este equipo emite un pulso de energía controlada (máx. 50 pulsos por minuto) que circula a través de hilos especiales de acero, que le dará una descarga al posible invasor, alejándolo de inmediato sin producirle daño. Seguramente también lo desalentará para un futuro intento. Este es un sistema que le brinda la posibilidad de que no tenga que lamentar nunca un robo, la invasión o el deterioro de un predio cercado eléctricamente. Este sistema le indicará sonoramente el momento exacto (con una demora menor a 4 segundos) en que el alambrado sea cortado, que el cercado sea puesto a tierra o que por algún motivo el Pulso Eléctrico de Alta

Tensión (en el cercado) caiga por debajo del nivel de seguridad preestablecido, y le permitirá tomar a Ud. Las medidas de seguridad pertinentes. La señal sonora se silenciará después de un breve tiempo sólo cuando se restablezca el funcionamiento correcto del cercado eléctrico. Asimismo, podrá detectar, si así lo necesita, el posible robo de la malla olímpica que está delante del cerco eléctrico. Se incluye una batería interna que le brinda una autonomía de hasta 72hs. sin suministro de energía eléctrica desde la red el cargador interno repone la carga de la batería.

FUENTE http://comprasegura.ec/productos.php?ncp=4414&pag=1&c=10&e=278

Equipos que forman el sistema

8 Vallas eléctricas de 1/3 de H.P. cada uno, de alto rendimiento, con detector de presencia de vehículo para evitar accidentes.

4 torniquetes de control de ingreso y salida

4 Paneles de control de accesos con 8 lectoras de proximidad.

PRESUPUESTO DEL SISTEMA. 36.000 Incluida mano de obra y materiales.

ESTE PRESUPUESTO SOLAMENTE INCLUYE EL CONTROL DE ACCESOS DE LAS GARITAS DE ENTRADA, PRINCIPAL Y DE EL AREA OPERATIVA.

Cada sistema que se necesite en diferentes áreas se debería adquirir independientemente, con la capacidad de usar el mismo tipo de tarjeta adquirido según requerimiento de la Fuerza.

Sistema de alarmas contra robo, asalto

El sistema de alarma estará instalado en cada una de las oficinas, bodegas, o dependencias de BASUIL. El sistema estará en la capacidad de controlar aperturas de puertas o accesos no deseados de cualquier persona. Además estará en condiciones de reportar una señal de activación de

cualquier detector de humo instalado o estación manual capaz de enviar una alarma de incendio. Tendrá la capacidad de enviar señales de asalto o emergencia no audibles a estación central de monitoreo.

El sistema cuenta con una fuente de poder y batería de respaldo para que pueda seguir operando en caso de corte de energía un mínimo de 6 horas. El corte de energía también se transmite a la central de monitoreo, como eventos de test, alarmas, aperturas, cierres, códigos de apertura y cierre, etc.

El sistema de control podrá ser activado y desactivado por medio de una clave (única e independiente para cada uno de los usuarios de cada sistema. Si no se pone la clave correcta en cada desactivación, el sistema entrara en alarma en un lapso de tiempo programado, haciendo sonar una sirena de altos decibeles en el sitio y al mismo tiempo enviara una señal digital del tipo de a la central de monitoreo, la cual procederá a procesar la señal y cumplir con los señal procedimientos de respuesta.

Cada panel de control consta de un comunicador digital que envía las señales a través de líneas telefónicas en códigos digitales a la central de monitoreo de alarmas, donde estas señales son recibidas y descifradas en la misma con un software especializado donde sale la información en claro del sitio, fecha, hora, dispositivo activado, etc.

Presupuesto del sistema

El costo de un sistema para cubrir una oficina es de 250 dólares.

El costo de un sistema para cubrir bodegas y oficinas 300 dólares.

A pesar que en este proyecto no se va a encargar del sistema contra incendios por existir un proyecto ejecutándose para este fin, se detalla los costos en caso de que un reparto lo necesite. El costo de un sistema para cubrir contra incendio, depende del número de detectores que se vaya a instalar con un costo promedio de 80 dólares por punto instalado, sin contar con el costo de tubería y cableado que asciende a un promedio de 4 dólares por metro de instalación.

Central de monitoreo de alarmas y C.C.T.V.

La CENTRAL RECEPTORA DIGITAL es un equipo de recepción de señales digitales a través de Línea telefónica, vía radio o mixta que recibe las señales enviadas por el comunicador que tienen los paneles de alarma instalados en cualquier establecimiento de BASUIL.

Cada uno de los sistemas estará monitoreado por la CENTRAL RECEPTORA DIGITAL, que estará operando 24 horas al día controlando la actividad de cada uno de los sistemas. Esta Central de monitoreo estará enlazada a una computadora con un Software CENTRAL-1 especializado el cual archivara toda la información recibida en cada unos de los sitios. Este software es un programa cerrado que no le permitirá al operador manipular la información, al contrario le exigirá que verifique cada una de las señales recibidas y grabe su acción en el computador al recibir cualquier señal de apertura o desactivación del sistema, cierre o activación del mismo. En cada apertura del sistema el operador estará en la obligación de verificar vía teléfono el código de entrada del usuario. Si no es válido enviara el personal de seguridad at sitio.

Equipos que forman el sistema

Sistema de alarma tipo:

Panel de control
Detectores infrarrojos / microonda de movimiento de doble tecnología, especial de alto rendimiento.
Contactos magnéticos para puestas metálicas, por local.
Detectores de humo y pulsadores manuales
Botonera de asalto.
Sirena de 30 W de altos decibeles con caja y tamper Switcher de protección por local.
Fuente de poder y batería de respaldo por local.

Receptora Digital con Software

10. Central de Monitoreo Digital, de un mínimo de 2 líneas telefónicas.
11. PC. Con el software CENTRAL-I en español.

Además el sistema estará compuesto por las pantallas de video que reciben las imágenes de las cámaras de televisión y el software de control de acceso de cada uno de los paneles instalados en la Base Naval.

PRESUPUESTO Incluido instalación y programación $ 11.800 USS. Dólares Americanos.

Sistema de detección perimétrica

Este sistema está a cargo de la protección perimetral de dos areas específicas:

12. Malla que colinda con FERTIZA. PERIFON
13. Área desprotegida que colinda con Autoridad Portuaria. PERIGUARD

El sistema PERIFON estará en capacidad de monitorear cualquier violación que exista en la malla que divide la base naval con Fertiza. La activación de este sistema por privación mandará una señal de alarma al cuarto de control, cuyo serial se podrá verificar con la cámara de televisión más cercana instalada en el sitio.

El sistema PERIGUARD estará en capacidad de monitorear cualquier violación en ingreso del perímetro que no se encuentra cercado, que colinda con Autoridad portuaria de Guayaquil. Si una persona cruza por este perímetro se enviara al cuarto de control una señal de alarma y de la zona violada. Este ingreso se podrá verificar con el sistema de C.C.T.V. con la cámara Autódromo que se encuentre más cerca al lugar.

Es importante aclara que en estos sectores contamos con dos cámaras móviles.

Los sistemas tendrán una tarjeta de control de corte de líneas, la cual será supervisada por un panel de control de alarma, la cual se mantendrá moni toreada por la central 24 horas al día.

Componentes del sistema

PERIFON

Panel de control
Cable de vibración

Repetidora y alimentadoras de señal.

PERIGUARD

Panel de control
Doble cable de señal de zonas de detección Repetidora de zonas.

PRESUPUESTO

PERIFON

Incluida mano de obra de instalación, programación y materiales $ 21.000

PERIGUARD

Incluida mano de obra de instalación, programación y materiales $ 36.000

MEJORA EN EL PROCESO ACTUAL

A continuación se presenta una propuesta de cómo deben desarrollarse los procedimientos analizados en el Capitulo 2.

INGRESO Y SALIDA DE PERSONAL Control

De Entrada Del Personal

1. El empleado solicita el ingreso de los datos al departamento de Recursos Humanos
2. En el Departamento de Recursos Humanos se ingresan los datos del empleado al sistema Biométrico.
3. En el Departamento de Recursos Humanos se Toman las Huellas Dactilares del empleado
4. Se almacenan los datos en un sistema que tiene una base de datos de DIGREH.
5. En el Departamento de Recursos Humanos se entrega un código de acceso al empleado
6. El empleado recibe el código de Acceso al sistema Biométrico

Control Hora de Entrada y Salida

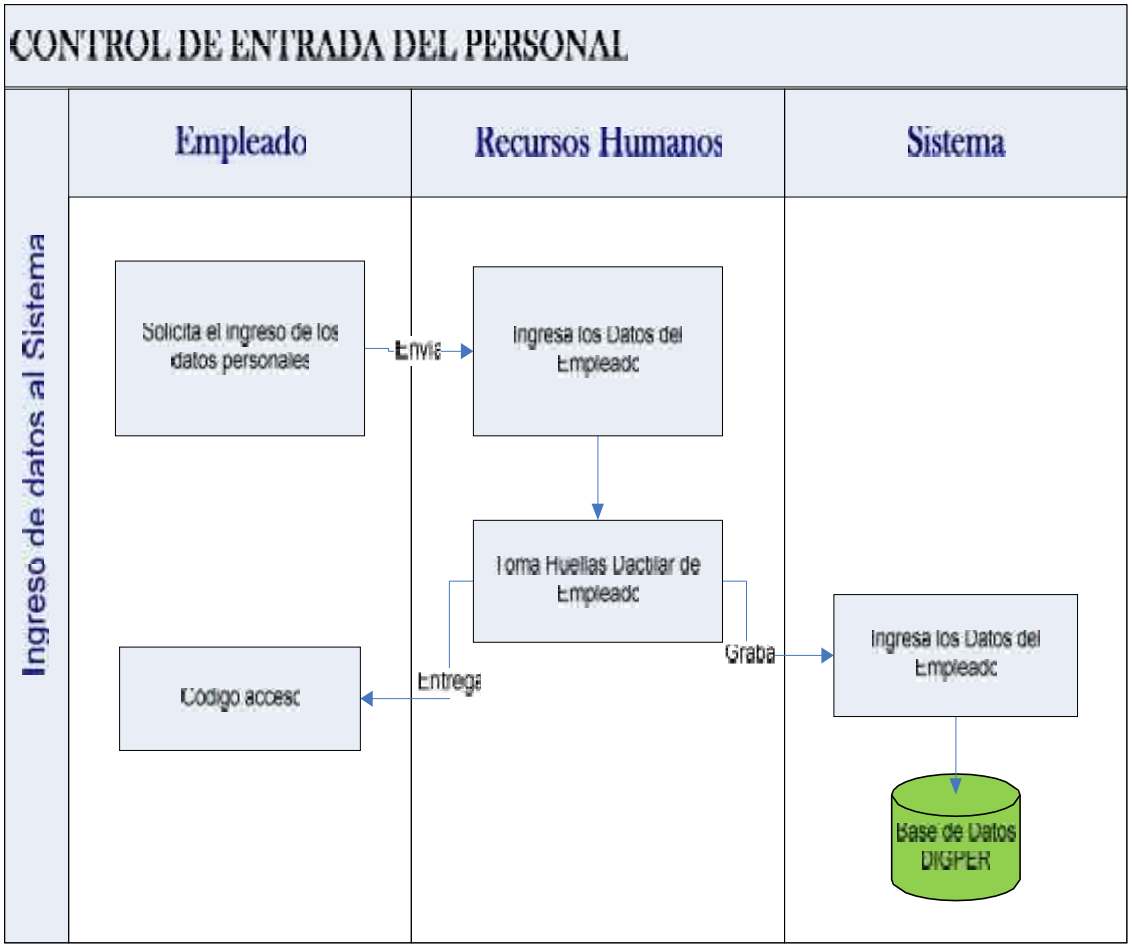
1. El empleado digita el Código acceso, presionar opción de entrada o salida y coloca el dedo en el Lector de Huella.
2. El sistema toma los datos de la base de DIGREH, analiza el código y la huella dactilar, para ver si es ingreso es correcto.
3. Si el ingreso es correcto entonces almacena los datos en la base de Datos de DIGREH.
4. Por no envía mensaje de error al usuario.

Control Entrada y Salida Visitantes

1. Entrega Cédula (al entrar al edificio)
2. El encargado de la guardia entrega tarjeta de Visita indicando el piso al que tiene acceso el invitado.
3. Al salir el visitante entrega la tarjeta de Visita al encargado de la guardia
4. Encargado de la guardia entrega la cedula al Visitante.

   Nota: La tarjeta le da permiso al visitante solo para el piso y departamento al que se dirige y a los accesos libres.

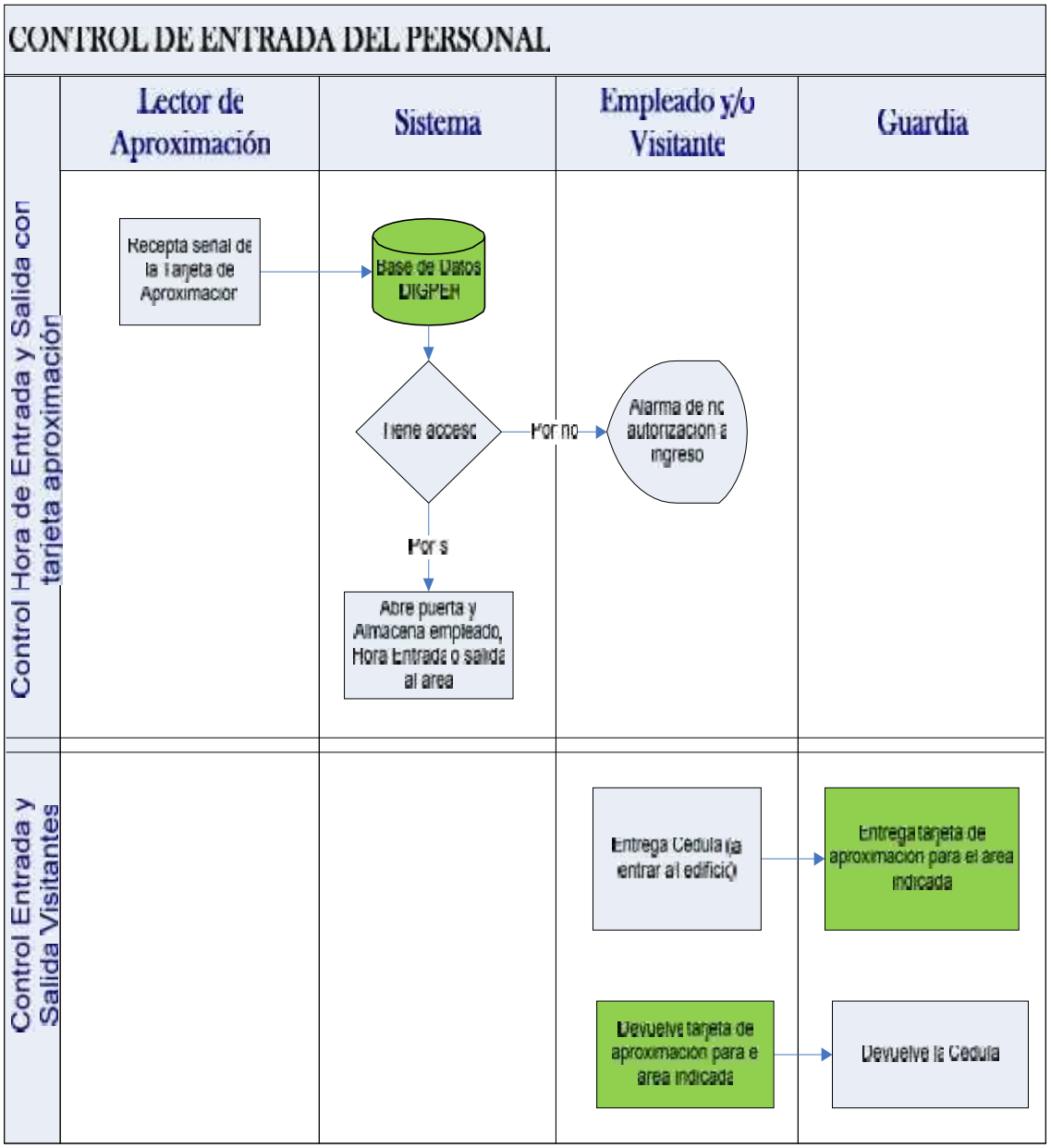
Control de Entrada y Salida del personal



Fuente: Grupo de trabajo (Colamarco, y otros, 2013)

Autor: Ing. Cecibel León Arreaga

Control de Ingreso y Salida del Personal Con Tarjeta de Aproximación



Fuente: Grupo de trabajo (Colamarco, y otros, 2013)

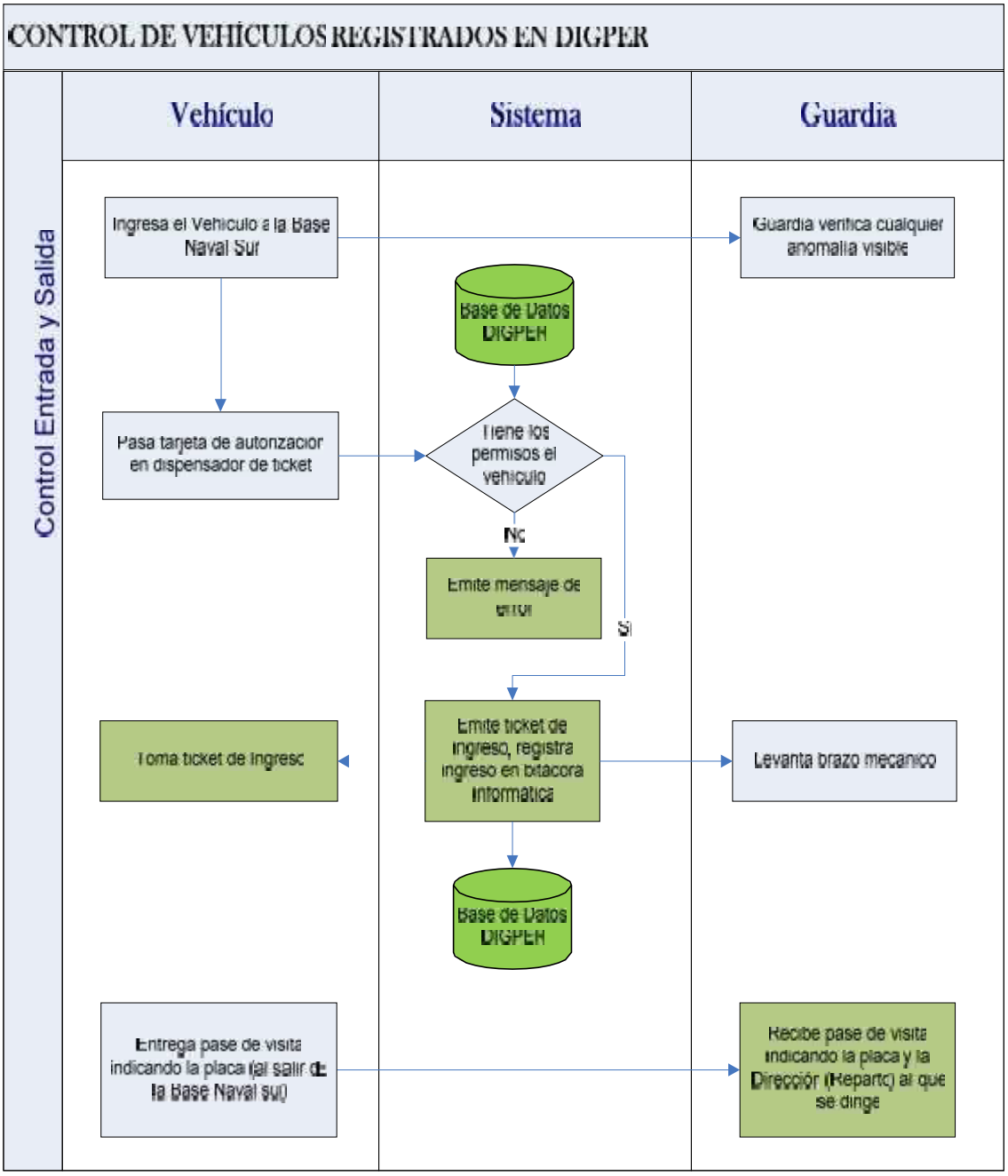
Autor: Ing. Cecibel León Arreaga

PROCESO PARA EL CONTROL DE VEHÍCULOS DE LA FUERZA NAVAL

Control Entrada y Salida

7. El Vehículo visitante ingresa al gate de la base.
8. El encargado de la guardia Vigila cualquier anomalía visible en el automóvil
9. Conductor pasa tarjeta de autorización en dispensador de tickets
10. El sistema evalúa si el vehículo tiene permisos. Tomando la información de la base de datos de DIGREH
11. En el caso que el vehículo no tiene permisos, se envía mensaje de error y el usuario debe ingresar como visitante
12. En caso de que si tenga permisos el vehículo, el sistema emite ticket de pase
13. El encargado de la guardia levanta el brazo mecánico. y el vehículo puede ingresar a la base.
14. En la salida el conductor entrega el ticket de ingreso al encargado de la guardia
15. El Vehículo puede salir de la base

Control De Vehículos



INGRESO A LOS SISTEMAS INFORMÁTICOS

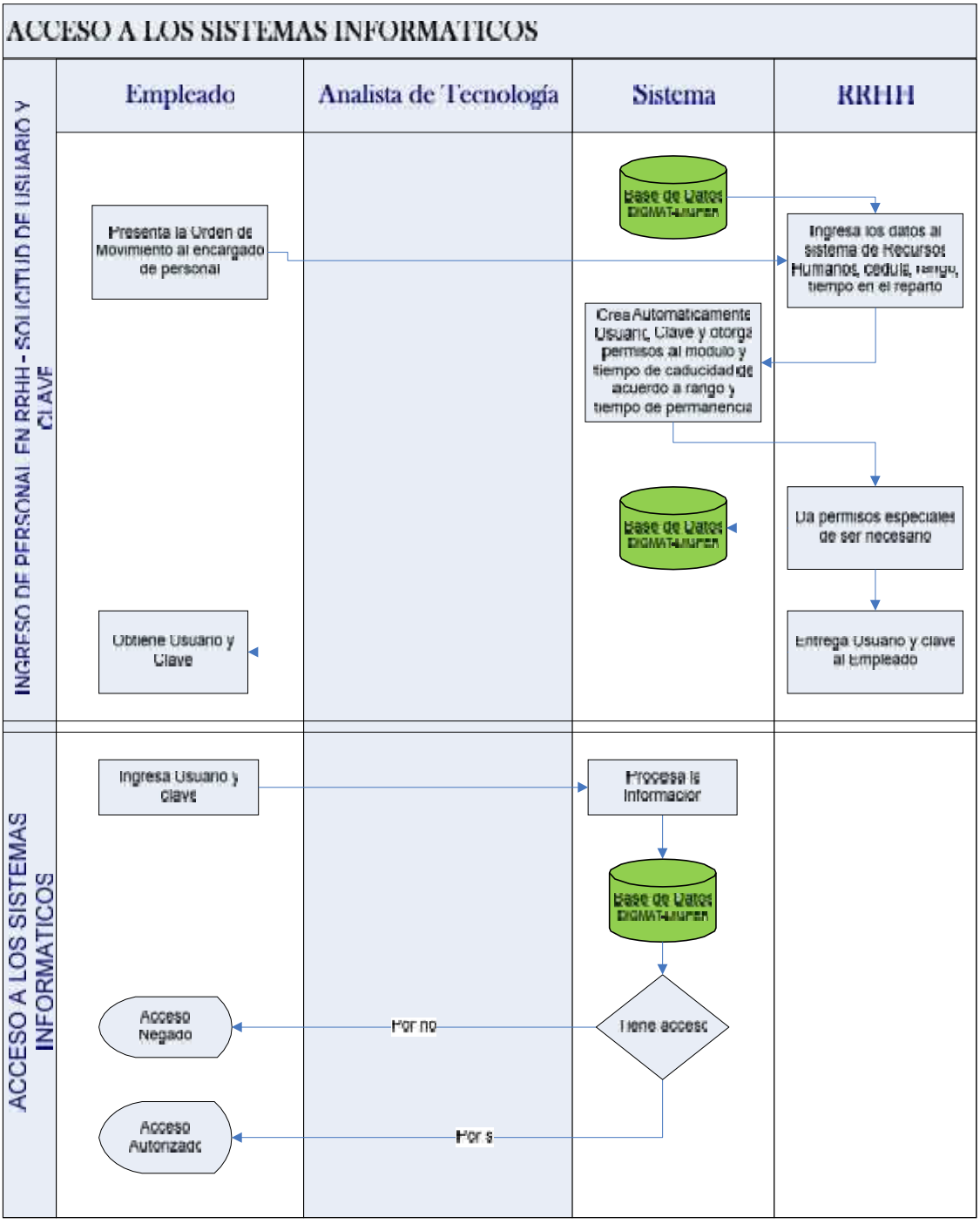
INGRESO DE PERSONAL EN RRHH

16. El empleado presenta la Orden de Movimiento al encargado de personal
17. El encargado de Recursos Humanos Ingresa los datos del empleado en el Sistema de Recursos Humanos
18. El sistema toma los datos de la Base de datos de DIGREH, revisa que no tenga asignado clave y usuario, si no lo tiene le asigna automáticamente, usuario y clave.
19. El encargado de Recursos humanos asigna permisos especiales en caso de ser necesario.
20. . El encargado de Recursos humanos entrega usuario y clave temporal al empleado
21. Recibe usuario y clave.

ACCESO A LOS SISTEMAS INFORMÁTICOS

1. Ingresa Usuario y clave
2. Procesa la Información,
3. Verifica en la base de Datos los permisos
4. Por si almacena datos de Hora y Fecha de ingreso en la base de Datos de Informix del Sistema Sislog.
5. Muestra mensaje de ingreso satisfactorio
6. Por No sale muestra mensaje de error.

Accesos A Sistemas Informáticos



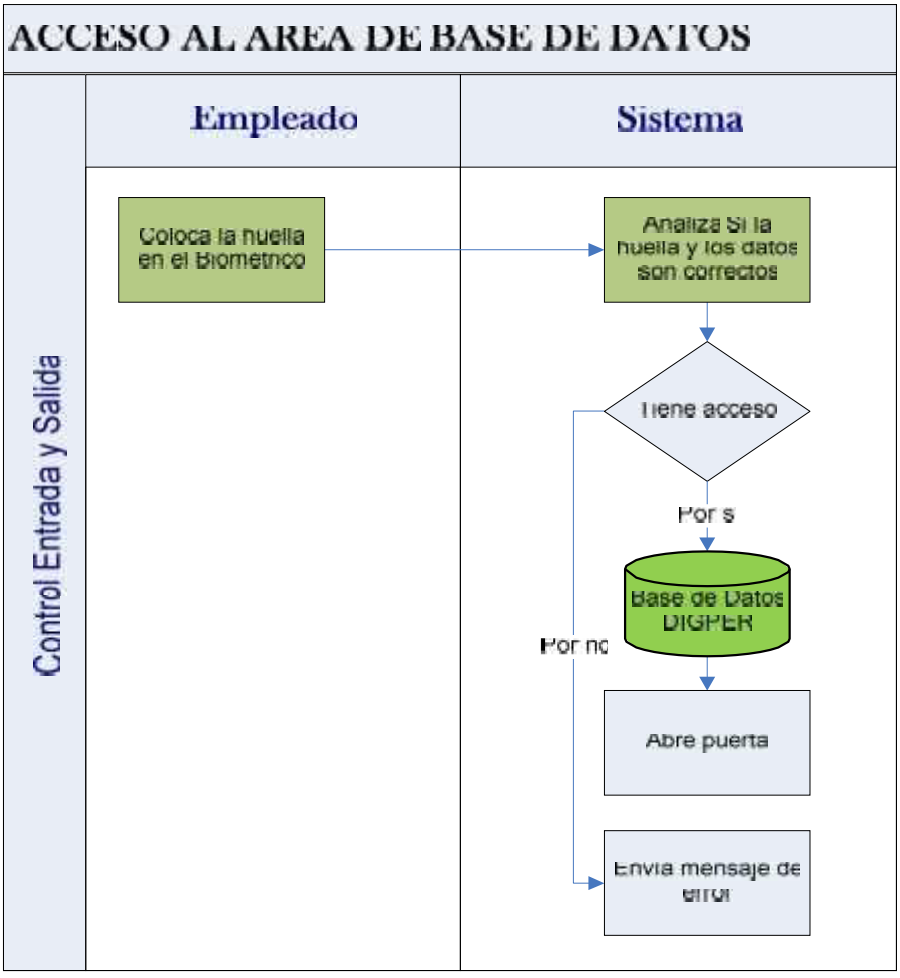
Fuente: Grupo de trabajo (Colamarco, y otros, 2013)

Autor: Ing. Cecibel León Arreaga

ACCESO AL ÁREA DE BASE DE DATOS

22. El empleado pasa coloca la huella en el lector biométrico
23. Analiza si los datos y las huella son corrector
24. Si tiene autorización almacena los datos de ingreso y/o salida en la Base de datos de DIGREH y abre la puerta
25. Por no tiene acceso no hace nada

Acceso A La Base De Datos



Fuente: Grupo de trabajo (Colamarco, y otros, 2013)

Autor: Ing. Cecibel León Arreaga

CAMBIOS EN SOFTWARE DE LA DIGMAT

Aprovechando que en la actualidad la Fuerza Naval se encuentra en un proceso de cambio de sus sistemas a plataformas Open Source, se deben agregar los cambios necesarios para la implementación del sistema integrado de seguridad.

Para el sistema de integrado de seguridad es necesario contar con el sistema de recursos humanos, puesto que de ahí se pueden obtener los datos necesarios para el 50% de la implementación del sistema.

Base de Datos del sistema Integrado de Seguridad de DIGMAT

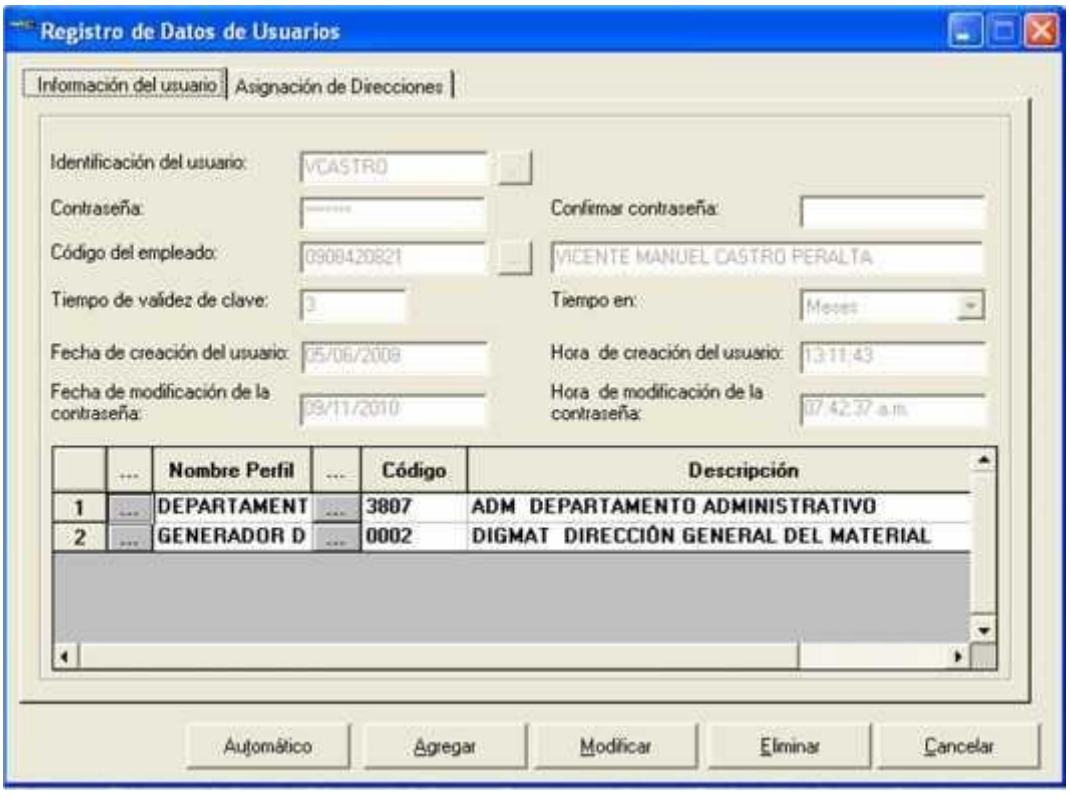
Para la elaboración del Modelo relacional de la Base de Datos del sistema integrado de seguridad, se tomó en consideración los estándares establecidos en el departamento de informática de la DIGMAT (CETEIN DIGMAT).

A continuación se muestra el modelo entidad-relación con los cambios necesarios. Cabe recalcar que solo se han mostrado las tablas que guardan relación directa con el sistema integrado de seguridad.

Principales Pantallas del sistema Biométrico de DIGMAT

Una vez estudiados los sistemas existentes en la Fuerza Naval, se decidió utilizar los software existentes, como los biométricos y las tarjetas de aproximación, que en este caso deberán ser adquiridos a la misma empresa y así utilizar el mismo software la toma de datos de ingreso y salida, estos datos deberán ser migrados a través de un proceso informático interno a la base de datos de seguridad y recursos humanos, Los datos genrales del Recurso Humano se tomaran de los sistema existentes a través de servicios, esto se refiere a consulta interna de datos que se comunican a través de internet, a continuación algunas de las pantallas del sistema.

Pantalla de ingreso a usuarios



Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

En esta pantalla se ingresarán los datos del usuario a partir de los datos obtenidos del sistema de recursos humanos. Y se le dará los perfiles a los sistemas y accesos de ingreso a los diferentes repartos de la Fuerza Naval.

Pantalla Usuarios (Asignación de Direcciones)

Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

Pantalla de ingreso de computadoras al sistema con el propósito de realizar las validaciones de ingreso, tanto a nivel de dominio informático del sistema operativo como de accesos a los mismos.

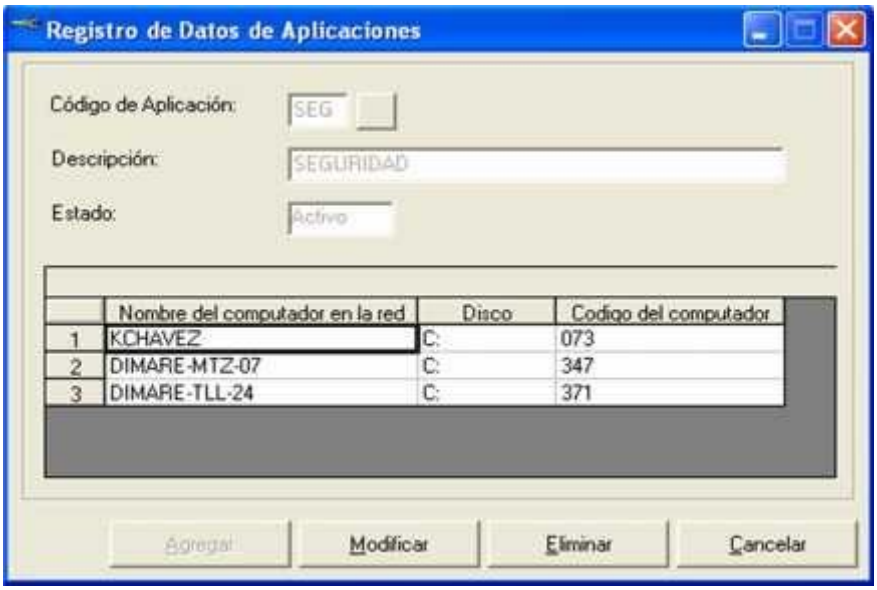
Registro de Empleados

Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

Registro de las diferentes aplicaciones o sistemas informáticos para centralizar los permisos.

Pantalla de Reportes

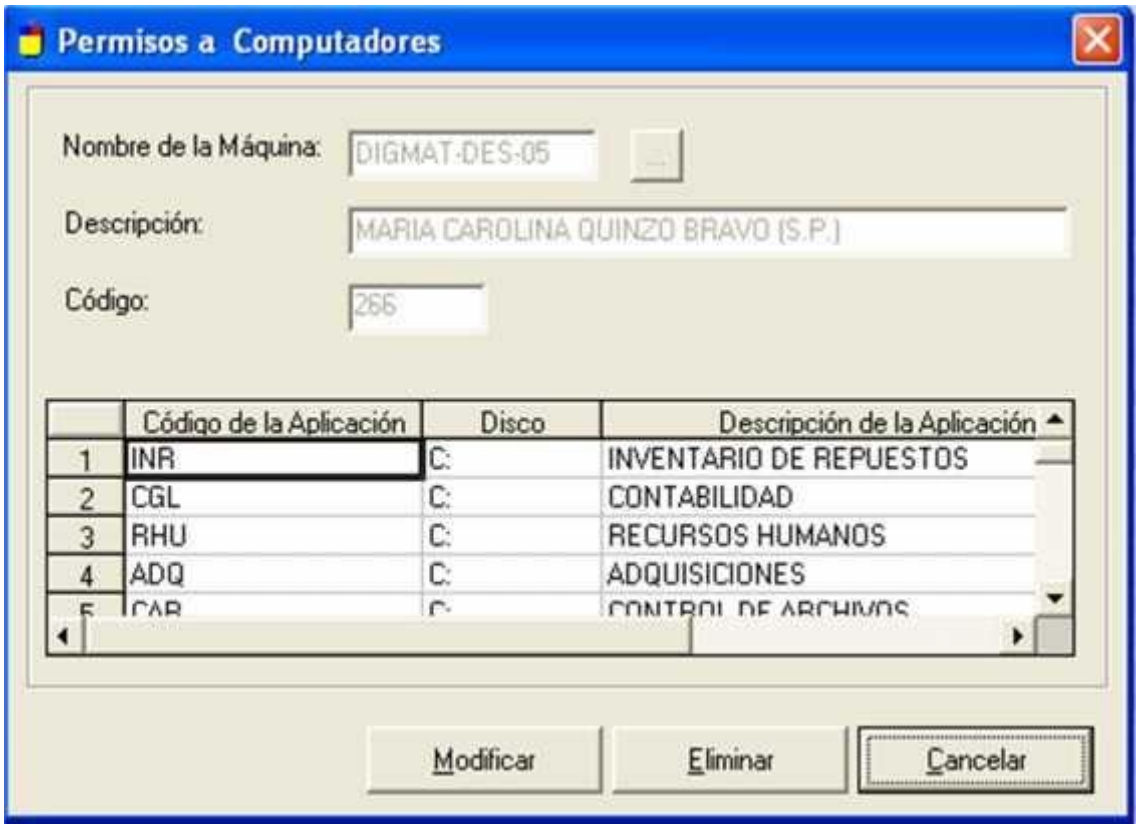


Fuente: Grupo de trabajo (Colamarco, y otros, 2013)

Autor: Ing. Cecibel León Arreaga

Permisos de los computadores a los sistemas según lo que requiera el perfil y/o el usuario.

Permisos a computadores

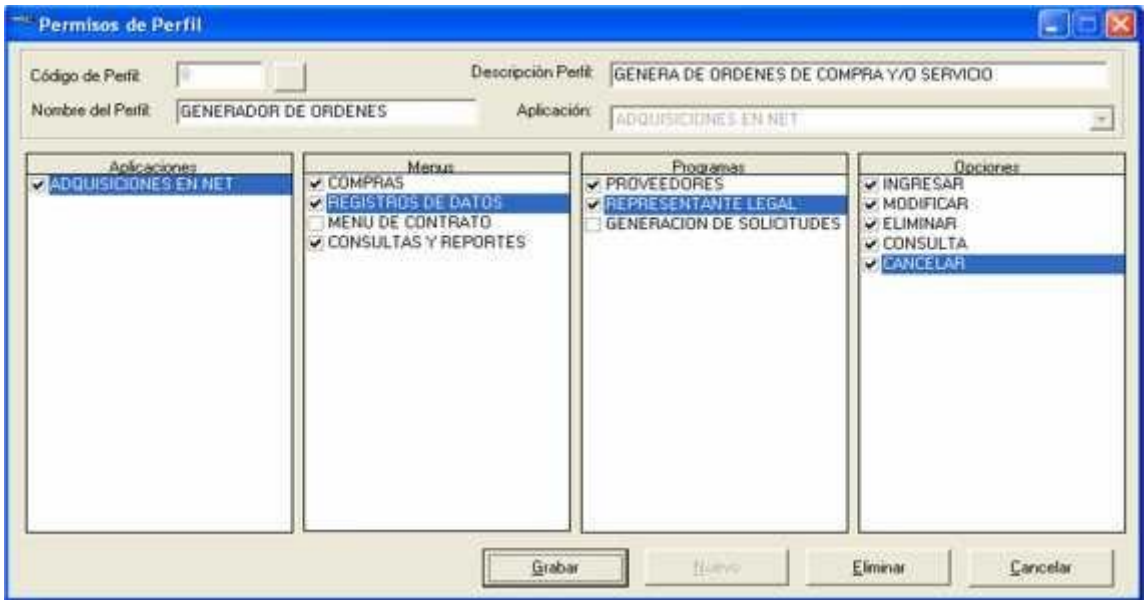


Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

Se crea perfiles por aplicaciones; luego estos perfiles son asignados a los usuarios.

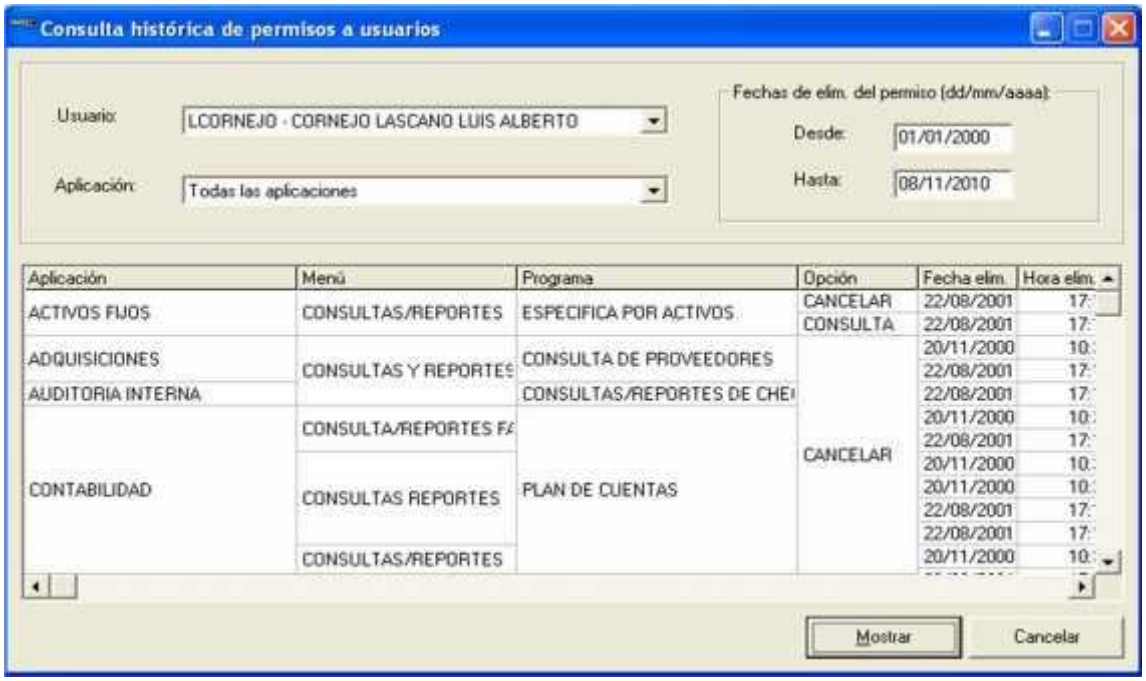
Ingreso de Perfiles de aplicaciones



Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

Consulta Histórica de permisos a usuarios



Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

Solicitud de Calificación de Seguridad de usuarios

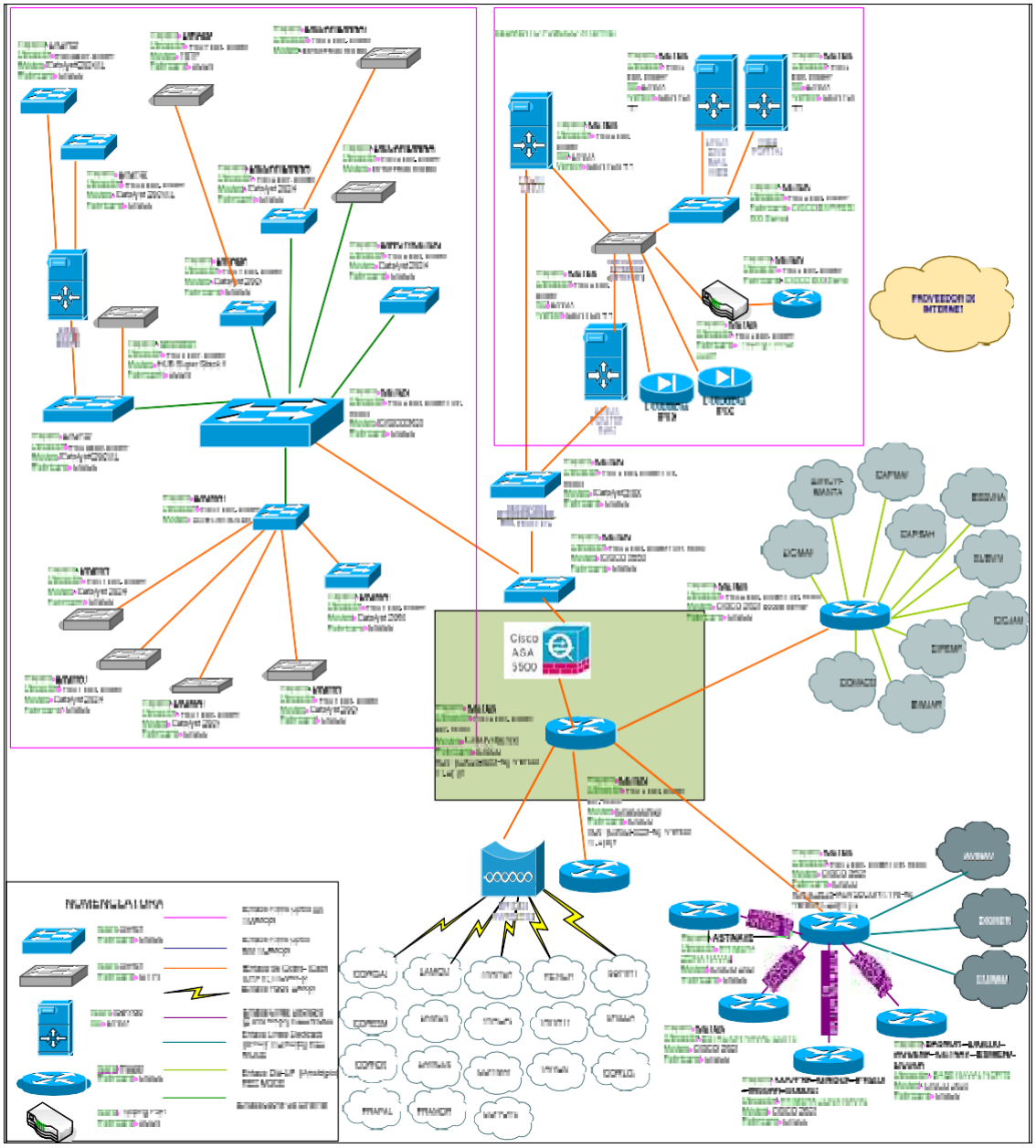
Fuente: Diseño en Base a Nuevos Procesos (León, 2012)

Autor: Ing. Cecibel León Arreaga

ANÁLISIS DE LA DE RED DE LA BASE NAVAL SUR

Debido a la importancia que tienen los sistemas computarizados, el área de redes ha venido cambiando y mejorando, es uno de los sectores en los que se ha prestado mayor atención en los últimos años

Diagrama De Interconexión De Repartos De La Base Naval Sur

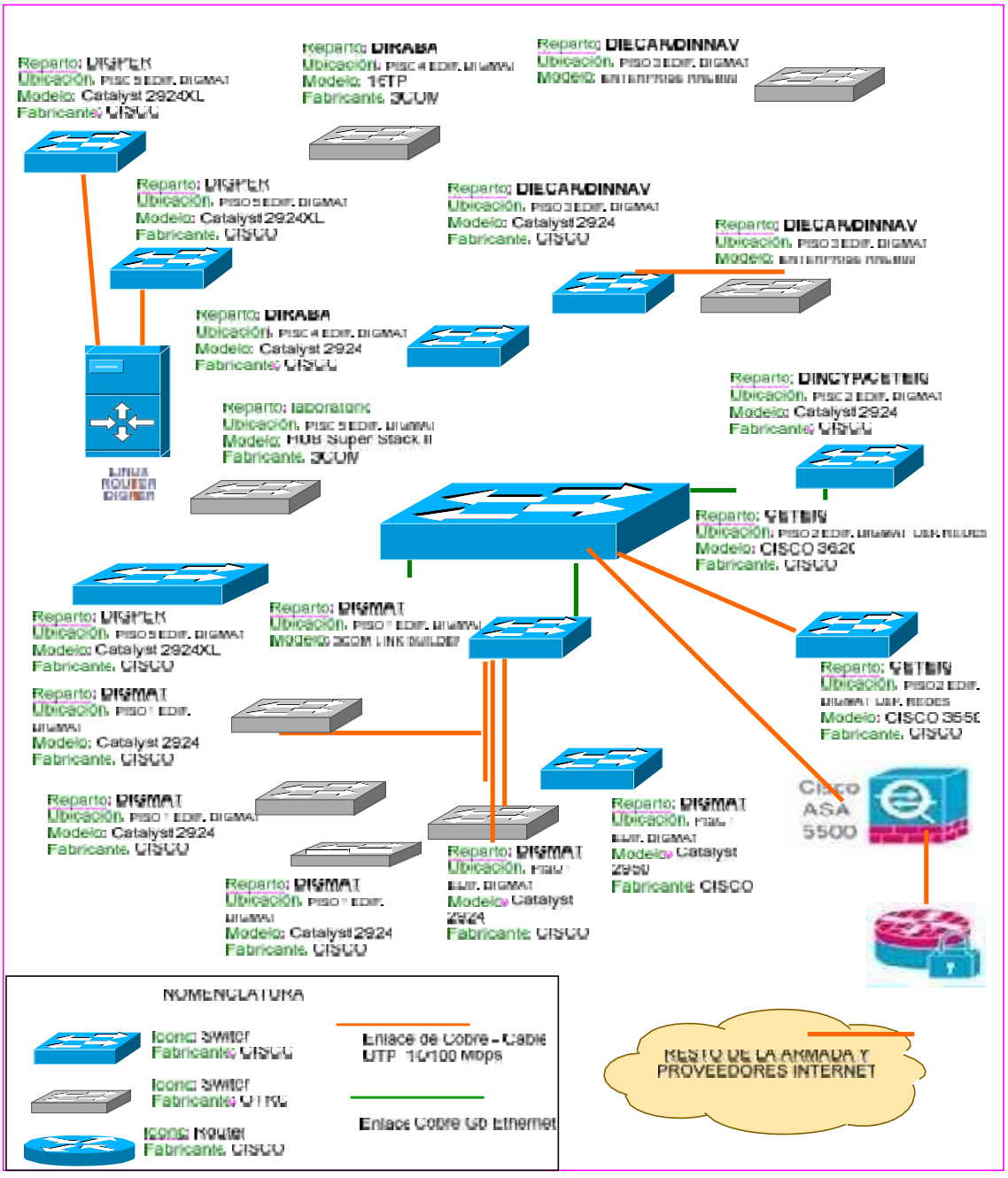


Fuente: Diseño de la Red de la Armada en Base a Medidas de Seguridad (Información, y otros, 2013)

Autor: Ing. Cecibel León Arreaga

DIAGRAMA DE RED DEL EDIFICIO DIGMAT PROPUESTO

Red Edificio DIGMAT



Fuente: Diseño de la Red de la Armada en Base a Medidas de Seguridad (Información, y otros, 2013)

Autor: Ing. Cecibel León Arreaga

CAMBIOS EN EL HARDWARE DE RED DE LA BASE NAVAL SUR

De acuerdo al diagnóstico realizado en el Capítulo 2, se observó que la red informática de la Base Naval sur tiene un inconveniente fundamental, y es la falta de seguridad interna; diciéndolo de otra forma, se cuida mucho la intromisión de extraños, pero recordemos que una de las principales falencias en toda seguridad es la que viene desde el interior cuando los usuarios, sin pretenderlo, dejan abiertos puertos o ingresan virus, dejan encendidas las máquinas, etc., poniendo en riesgo la seguridad de la información. Por esto es de suma importancia determinar los sistemas de seguridad entre las redes LAN que forma la red WAN de la Fuerza Naval del Ecuador.

Equipos De Red Que Deben Implementarse En La Base Naval Sur

Primero se hablará de lo que es la tecnología de autodefensa de cisco ASA 5500.

Cualquier empresa que dependa de su red, necesita una seguridad sólida. Los Dispositivos de Seguridad Adaptativos de Cisco ASA Serie 5500 ofrecen una seguridad de última generación con la flexibilidad necesaria para satisfacer las necesidades de su compañía a medida que ésta crece y cambia.

La red de autodefensa de cisco es escalable y puede aplicarse a empresas de cualquier tamaño

Los Dispositivos de Seguridad Adaptativos de Cisco ASA Serie 5500 soportan:

- *Personalización: Personalice la seguridad según sus necesidades de acceso específicas y sus políticas comerciales.*
- *Flexibilidad: Conforme su negocio crezca y necesite cambios, podrá agregar fácilmente capacidades o actualizar de un dispositivo a otro.*
- *Seguridad avanzada: Aproveche los últimos avances en seguridad de contenidos, cifrado, autenticación de identidad, autorización y prevención de intrusiones.*

- *Simplicidad: Utilice un dispositivo diseñado para ser fácil de instalar, gestionar y supervisar.*
- *Redes avanzadas: Configure redes privadas virtuales (VPN) que proporcionen a los trabajadores remotos y móviles un acceso seguro a los recursos de la compañía o establezca VPN entre partners, otras oficinas o empleados basadas en roles.*
  Al mantener su red segura y protegida, los empleados podrán acceder siempre a ella desde su ubicación. Los Dispositivos de Seguridad Adaptativos de la ASA Serie 5500 de Cisco son su primera y mejor línea de defensa

La serie Cisco ASA 5500 es una familia de dispositivos de seguridad multifunción de alto rendimiento que proporciona convergencia de firewall, IPS, antivirus de red y servicios VPN. Entre otras características cabe destacar las siguientes:

- *Funciones VPN y seguridad comprobadas en el mercado: un firewall muy completo de alto rendimiento, IPS, antivirus de red y las tecnologías de VPN IPSec/SSL ofrecen una robusta seguridad de las aplicaciones, control de acceso basado en usuarios y en aplicaciones, mitigación de gusanos y virus, protección contra software malicioso y conectividad remota de usuario/sitio.*
- *Exclusiva arquitectura de servicios adaptables de identificación y mitigación: permite a las empresas adaptar y ampliar el perfil de los servicios de seguridad de la serie Cisco ASA 5500 mediante políticas de seguridad específicas del flujo que adaptan las necesidades de seguridad a las necesidades de las aplicaciones y paralelamente brinda un alto rendimiento y la posibilidad de ampliar los servicios de seguridad a través de los módulos de servicios de seguridad (SSM) que puede instalar el usuario.*

- *Menores costos de implementación y operación: Los equipos multifunción permiten normalizar la plataforma, la configuración y la administración, con lo cual se reducen tanto los costos de implementación como los operativos.*

Figura 4.17

Cisco ASA Serie 5500

Fuente: (CISCO)

Autor: CISCO

La Serie Cisco ASA 5500 integra una combinación de tecnologías en una única plataforma para la detección proactiva de amenazas y ataques que asedian las redes de nuestros clientes. Detiene los ataques antes de que entren en la red, controla la actividad y provee conectividad VPN flexible.

El resultado es una herramienta perfecta para todo tipo de redes corporativas, reduciendo el coste y la complejidad asociados a la instalación de productos con el mismo nivel de seguridad.

Con la serie 5500 de Cisco ASA podremos proteger de un modo más efectivo y eficiente las redes de nuestros clientes gracias a la combinación de la última tecnología proveniente de los PIX 500, la serie IPS 4200 y la serie VPN 3000 de Cisco Systems añadiendo, además, el nuevo equipamiento Anti-X.

- *Firewall de Alto rendimiento*
- *Conectividad VPN de alto rendimiento (IPSec y SSL)*
- *Sistema de prevención de intrusiones*
- *Anti-X*

Para implementar este tipo de seguridad se requiere:

Características de Cisco ASA 5500

Cisco ASA 5500 Series Model/License Cisco ASA 5500 Series Modelo / licencia	
Cisco ASA 5585-X con la SSP-10	
Ubicación de la red	Internet Edge, Campus Borde de Internet, Campus
Resumen de rendimiento	
Firewall Throughput 1 Servidor de seguridad de un rendimiento	2 Gbps (multi-protocol), 4 Gbps (max)
Número máximo de conexiones de Firewall	**750,000**
Número máximo de conexiones Firewall / Segunda	50,000
Los paquetes por segundo (64 bytes)	1,500,000
Máximo Rendimiento 3DES/AES VPN 2	1 Gbps
Sitio máximo a sitio remoto y sesiones VPN de acceso	5,000
Máximo SSL VPN sesiones de usuario	5,000
Incluido SSL VPN sesiones de usuario	2
Resumen técnico	
Memoria	6 GB (SSP-10) 12 GB (SSP-10 and IPS SSP-
Mínima del sistema Flash	2 GB 2 GB

Integrado Puertos	8-10/100/1000, 2-10 GE SFP + (con ASA5585-Sec-Pl de licencia), 2-10/100/1000 gestión
Máximo Virtual Interfaces (VLAN)	250
Posibilidades de ampliación	
SSP de expansión	1- IPS SSP
SSP compatibles	IPS SSP-10
De prevención de intrusiones	Sí (con IPS SSP)
Mitigación de amenazas simultáneas Rendimiento (Mbps) (IPS Servicios + Firewall)	2 Gbps
Features Características	
Cisco Adaptive Security Appliance Software versión (la última)	8.2.3
La capa de aplicación de servicios de firewall	Sí
Capa 2 cortafuegos transparente	Sí
Contextos de seguridad (incluidos / 3 como máximo)	2 / 50
GTP / GPRS de Inspección 3	Sí
Alta disponibilidad de la ayuda 4	A / A y A / S
SSL y VPN IPsec Servicios	Sí
VPN de clústeres y equilibrio de carga	Sí
Avanzada de Evaluación de punto final 3	Sí

Cisco ASA 5585-X con la SSP-10

Fuente: (CISCO)

Fuente: (CISCO)

Autor: CISCO

Características de Cisco RV016 Cisco Small Business Routers

Router para VPN con varias conexiones WAN Cisco RV016 Cisco Small Business Routers

WAN Cisco RV016 Cisco Small Business Routers

- Acceso remoto seguro en el corazón de la red de las pequeñas empresas
- Lo más destacado
- Conectividad para varias WAN: se pueden configurar hasta 7 puertos para conseguir redundancia de conexión y equilibrio de carga
- 16 puertos Ethernet conmutados de 10/100
- Completas funciones VPN IPsec para un máximo de 100 conexiones remotas

- Firewall con inspección de estado de paquetes (SPI) avanzada para ayudarle a preservar la seguridad de su red

Características

- Firewall SPI para máxima seguridad
- Switch 10/100 de 16 puertos que admite interfaz dependiente del medio (MDI) e interfaz cruzada dependiente del medio (MDI-X), y una capacidad de transferencia de hasta 200 Mbps por puerto
- 5 de los 16 puertos se pueden configurar como puertos WAN/LAN
- Dos puertos WAN dedicados para conectividad a Internet de carga equilibrada
- Análisis del correo electrónico y URL dinámicas a través del Servicio de Seguridad Trend Micro ProtectLink Gateway (opcional)
- Capacidad de VPN IPsec (IP security, seguridad de IP) completa mediante el cifrado DES (Data Encryption Standard, norma de cifrado de datos) y 3DES (triple DES)
- Compatibilidad con los algoritmos de autenticación MD5 y SHA.
- Hasta 100 túneles de IPsec VPN simultáneos permitidos
- Gestión a través de Internet, protocolo SNMP (Simple Network Management Protocol, protocolo de gestión de red simple) y asistente de configuración para facilitar la conexión a los administadores
- Capacidades de gestión del ancho de banda para ofrecer mejor QoS (Quality of Service, calidad de servicio)
- Hasta 50 usuarios de QuickVPN admitidos

Fuente: (CISCO)

Autor: CISCO

Características de Cisco CS-MARS-200 Security Monitoring Analysis and Response System

Cisco CS-MARS-200 Security Monitoring Analysis and Response System
 La supervisión de la seguridad de Cisco, en análisis y respuesta (Cisco Security MARS) es una solución basada en dispositivos, todo incluida que proporciona una visión sin precedentes y el control de su implantación de seguridades existentes. Parte del ciclo de vida de gestión de seguridad de Cisco, MARS de seguridad de Cisco permite a las organizaciones de seguridad y de red para identificar, gestionar y contrarrestar las amenazas de seguridad. Trabaja con su red existente y las inversiones en seguridad para identificar, aislar y recomienda extracción precisa de elementos problemáticos. También ayuda a mantener el cumplimiento de las políticas internas y puede ser una parte integral de su solución de cumplimiento de normas en general. REFURB CS-MARS 200 4RU 10000 EPS 1TB RAID 10 DEVICE TYPE NETWORK MONITORING DEVICE ENCLOSURE TYPE RACK-MOUNTABLE - 4U APPROXIMATE DIMENSIONS (WXDXH) 25.6 IN HARD DRIVE 1 TB OPTICAL STORAGE DVD-ROM PORTS QTY 2 DATA LINK PROTOCOL ETHERNET, FAST ETHERNET, GIGABIT ETHERNET FEATURES FIREWALL PROTECTION
Cisco Número de pieza (modelos locales Contralor) Seguridad de Cisco MARS 200 (CS-MARS-200-K9)

Eventos / Sec.1	10.000

NetFlows / Sec	300.000
Almacenamiento	1.000 GB RAID 10 intercambiables en caliente
Unidad de rack	4 x 25,6 pulg RU
Poder	500W de doble redundancia, 120/240V detector magnético

Sesión dinámica basada en correlación

- Red de detección de anomalías en la base, incluyendo Cisco NetFlow
- Comportamiento de eventos basado y basado en normas correlación
- Amplia incorporados y normas definidas por el usuario
- Automatización NAT normalización

Topology Discovery

- Nivel 3 y Nivel 2 routers, switches y cortafuegos
- Red de IDS palas y equipos
- Manual y programada descubrimiento
- Secure Shell (SSH), SNMP, Telnet y específicas del dispositivo de comunicaciones

La agregación de red inteligente de eventos y rendimiento de procesamiento

Cisco Security MARS obtiene inteligencia de la red mediante la comprensión de la topología y configuración de los dispositivos de los enrutadores, conmutadores y firewalls, y por un perfil de tráfico de red. El sistema de la función de descubrimiento de red integrada construye un mapa de topología que contiene la configuración de dispositivos y las políticas actuales de seguridad, lo que le permite modelar los flujos de paquetes a través de su red. Dado que el aparato no opera en línea y hace un uso mínimo de agentes de software existentes, hay poco impacto en la red o el rendimiento del sistema.

El aparato central agregados los registros y eventos de una amplia gama de dispositivos de red populares (como routers y switches), dispositivos de seguridad y aplicaciones (tales como cortafuegos, sistemas de detección de intrusos [IDS],

escáneres de vulnerabilidad, y las aplicaciones de antivirus), los anfitriones (por ejemplo como Windows, Solaris y Linux syslogs), aplicaciones (bases de datos, servidores Web y servidores de autenticación), y el tráfico de red (tales como Cisco NetFlow).

Cisco Context Correlation

Como los acontecimientos y se reciban los datos, la información se normaliza en contra de la topología, configuración de los dispositivos descubiertos, la misma fuente y las aplicaciones de destino a través de Network Address Translation límites [NAT].Correspondiente eventos se agrupan en sesiones en tiempo real. Sistema y reglas de correlación definidas por el usuario son aplicados a varias sesiones para identificar los incidentes. Cisco Security MARS buques con un completo complemento de reglas predefinidas, actualizada con frecuencia por Cisco, que identifican la mayoría de escenarios de ataque combinado, los ataques de día cero y gusanos. Un marco regla de definición gráfica simplifica la creación de reglas personalizadas definidas por el usuario para cualquier aplicación. ContextCorrelation reduce significativamente los datos en bruto caso, facilita la priorización de respuesta, y maximiza los resultados de las contramedidas desplegadas.

Fuente: (CISCO)

Autor: CISCO

CRONOGRAMA DE ACTIVIDADES

En base a lo antes expuesto se realizó el proyecto con los recursos y actividades necesarias para poder cumplir con las expectativas de este trabajo.

RECURSOS A UTILIZAR

Recursos a Utilizar

Cisco CS-MARS-200 Security Monitoring Analysi	Material	C		22.000,00 $
Router para VPN con varias conexiones WAN Ci	Material	R		400,00 $
Cisco ASA 5500 Series Model/License Cisco AS.	Material	C		7.500,00 $
Cambios en Base de Datos (personal de DIGMA	Material	C		0,00 $
Cambios en Software (personal de DIGMAT)	Material	C		0,00 $
Servidor para almacenamiento de imágenes	Material	S		2.000,00 $
Servidor de contingencia para almacenamiento c	Material	S		2.000,00 $
Pc para Garitas	Material	P		750,00 $
Equipos de TV para circuito cerrado	Material	E		1.500,00 $
Autodomos PTZs de 1/3 a color con Zoom de un	Material	A		1.386,00 $
cámaras a color con lente varifocal, autoiris, blin	Material	c		140,00 $
Sistema de video grabación digital con disco dur	Material			2.600,00 $
Sistema de video transmisión a través de fibra óp	Material	S		50,00 $
Mano de Obra por instaliciónd e 14 Cámaras y c	Material	M		300,00 $
Vallas eléctricas de 1/3 de H.P. cada uno, de alto	Material	V		2.700,00 $
torniquetes de control de ingreso y salida, leen ta	Material	t		1.600,00 $
Paneles de control de accesos con 8 lectoras de	Material	P		250,00 $
Instalación y software de acceso	Material	I		0,00 $
Tarjetas de proximidad	Material	T		7,00 $
Panel de control (se usaría el mismo de circuito c	Material	P		0,00 $
Detectores infrarrojos / microonda de movimiento	Material	D		250,00 $
Contactos magnéticos para puestas metálicas, p	Material	C		50,00 $
vallas puerto	Material	v		21.000,00 $
vallas fertiza	Material	v		36.000,00 $
Personal de Contratos	Trabajo	CON	100%	8,00 $/hora
Personal de plan Director	Trabajo	PLA	100%	8,00 $/hora
Personal de Dirección de Abastecimiento	Trabajo	DIRABA	200%	8,00 $/hora
Personal DIGMAT-DES)Desarrollo Institucional)	Trabajo	DES	300%	8,00 $/hora
Personal de Inspectoría de la Fuerza Naval	Trabajo	INSGAR	100%	8,00 $/hora
Personal Dirección de Tecnología de la Informaci	Trabajo	DIRTIC	400%	8,00 $/hora
Personal de Seguridad Institucional de la Armada	Trabajo	SECGAR	200%	8,00 $/hora
Fiscalizadores	Trabajo	F	300%	8,00 $/hora
Personal de Dirección de Ingenieria Civil y Portua	Trabajo	DINCYP	300%	8,00 $/hora
Personal de Seguridad Institucional de la Armada	Trabajo	P	100%	0,00 $/hora

Fuente: Investigación en el Mercado (León, 2012)

Autor: Ing. Cecibel León Arreaga

ACTIVIDADES A REALIZAR

En base a las actividades se ha realizado un cronograma de actividades el mismo que se muestra a continuación:

Lista de Actividades con los datos básicos del proyecto

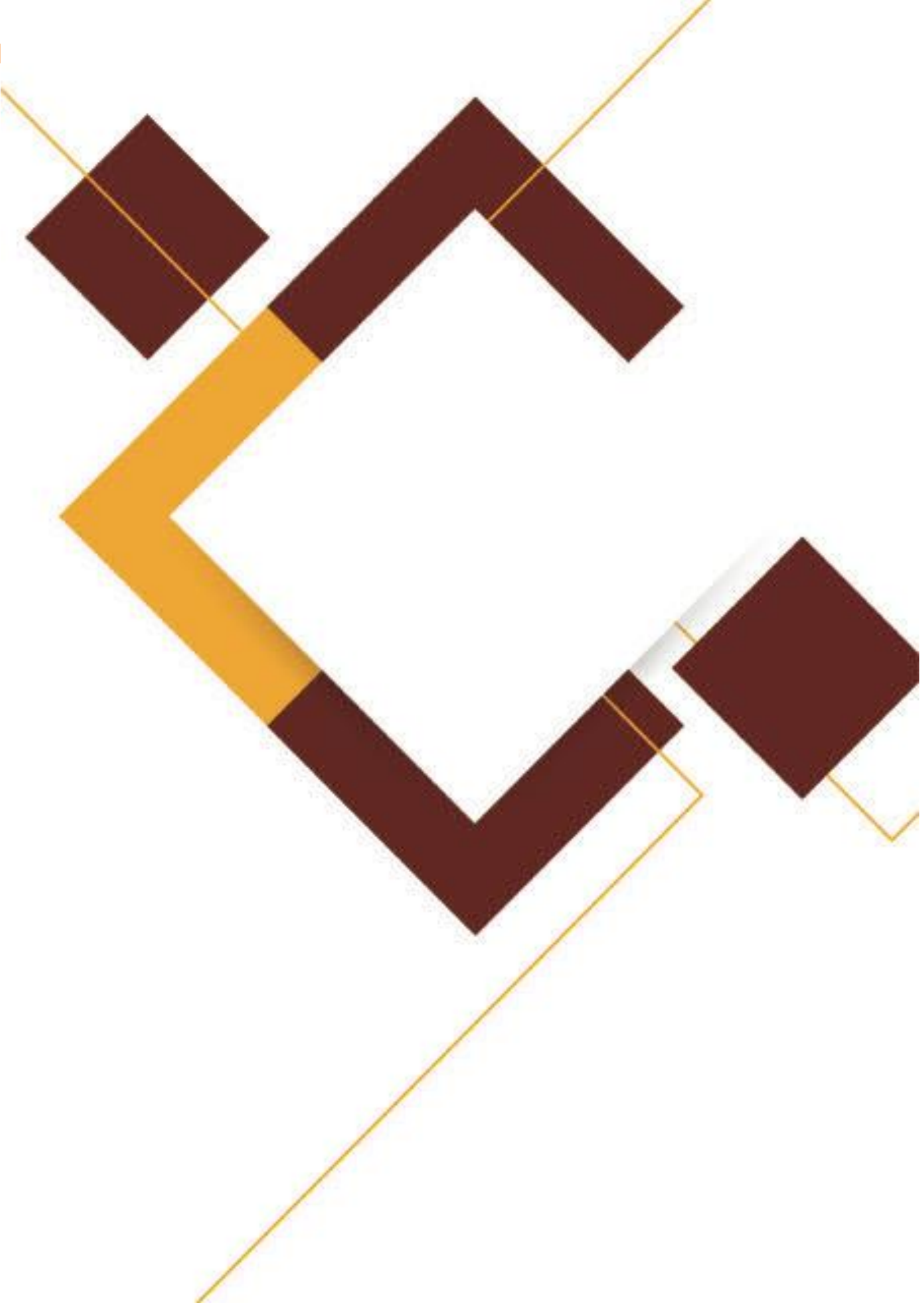
	Nombre de tarea	Duración	Comienzo	Fin	ce	Nombres de los recursos
1	**Seguridad**	**145 días**	**lun 07/01/13**	**vie 26/07/13**		
2	**Presentar un proyecto de Seguridad Integral automatizada al alto mando.**	**60 días**	**lun 07/01/13**	**vie 29/03/13**		
3	Elaborar Proyecto de seguridad integral automatizada	20 días	lun 07/01/13	vie 01/02/13		Personal de Contratos
4	Conseguir los recursos necesarios para poner en marcha el proyecto.	20 días	lun 04/02/13	vie 01/03/13	3	Personal de plan Director
5	Realizar el programa de adquisición para que sea aprobado por el gobierno	20 días	lun 04/03/13	vie 29/03/13	4	Personal de Dirección de Abastecimiento
6	Determinar los responsables del proyecto por áreas	5 días	lun 04/03/13	vie 08/03/13	4	Personal DIGMAT-DES)Desarrollo Institucional)
7	Realizar un programa de promoción del sistema para darlo a conocer a todos los miembros	10 días	lun 07/01/13	vie 18/01/13		Personal DIGMAT-DES)Desarrollo Institucional)
8	**Financiamiento:**	**20 días**	**lun 07/01/13**	**vie 01/02/13**		
9	Realizar un estudio de las diferencias con las Armadas de Sudamérica y Latinoamérica y la del Ecuador para demostrar la necesidad de mejorar el sistema de seguridad.	10 días	lun 07/01/13	vie 18/01/13		Personal DIGMAT-DES)Desarrollo Institucional)
10	Demostrar con estudios respecto de un posible atentado para demostrar la necesidad de la mejora de la seguridad Institucional, esto puede hacerse con ayuda de la Dirección de Inteligencia Institucional.	10 días	lun 21/01/13	vie 01/02/13	9	Personal DIGMAT-DES)Desarrollo Institucional)
11	**Publicidad Y Motivación**	**30 días**	**lun 04/02/13**	**vie 15/03/13**		
12	Realizar un programa de capacitación y promoción del Plan de Seguridad Institucional, y de la necesidad del mismo al mando medio para concientizarlo sobre el seguimiento de los procesos y procedimientos de seguridad.	30 días	lun 04/02/13	vie 15/03/13	10	Personal DIGMAT-DES)Desarrollo Institucional)
13	Realizar programas de simulacros de infiltraciones cuyos resultados sean expuestos al medio mando para que ellos sientan el peso de su responsabilidad para que no se den infiltraciones reales	30 días	lun 04/02/13	vie 15/03/13	10	Personal de Inspectoría de la Fuerza Naval,Personal DIGMAT-DES)Desarrollo Institucional)

	Nombre de tarea	Duración	Comienzo	Fin	ce	Nombres de los recursos
14	**Implementación del proyecto de seguridad Integral**	**95 días**	**lun 18/03/13**	**vie 26/07/13**		
15	Realizar concursos de adjudicación de compras y contrataciones	30 días	lun 18/03/13	vie 26/04/13	13	rsonal de Contratos,Personal de Dirección de Abastecimiento
16	**SEGURIDAD DE RED**	**5 días**	**lun 29/04/13**	**vie 03/05/13**		
17	Instalación de Cisco CS-MARS-200 Security Monitoring Analysis and Response System	5 días	lun 29/04/13	vie 03/05/13	15	Cisco CS-MARS-200 Security Monitoring Analysis and Response System[1],Personal Dirección de Tecnología de la Información
18	Instalación de Router para VPN con varias conexiones WAN Cisco RV016 Cisco Small Business Routers	5 días	lun 29/04/13	vie 03/05/13	15	Router para VPN con varias conexiones WAN Cisco RV016 Cisco Small Business Routers[1],Personal Dirección de Tecnología de la Información
19	Instalación de Cisco ASA 5500 Series Model/License Cisco ASA 5500 Series Modelo / licencia	5 días	lun 29/04/13	vie 03/05/13	15	Cisco ASA 5500 Series Model/License Cisco ASA 5500 Series Modelo / licencia[1],Personal Dirección de Tecnología de la Información
20	**CAMBIO DE SOFTWARE**	**40 días**	**lun 06/05/13**	**vie 28/06/13**	**19**	
21	Cambios en Base de Datos (personal de DIGMAT)	10 días	lun 06/05/13	vie 17/05/13	19	Personal Dirección de Tecnología de la Información
22	Cambios en Software (personal de DIGMAT)	40 días	lun 06/05/13	vie 28/06/13	19	Personal Dirección de Tecnología de la Información
23	Instalación de Servidor para almacenamiento de imágenes	5 días	lun 06/05/13	vie 10/05/13	19	Personal Dirección de Tecnología de la Información,Servidor para almacenamiento de imágenes [1]
24	Instalación de Servidor de contingencia para almacenamiento de imágenes	5 días	lun 13/05/13	vie 17/05/13	23	Personal Dirección de Tecnología de la Información,Servidor de contingencia para almacenamiento de imágenes [1]
25	Instalación de Pc para Garitas	5 días	lun 20/05/13	vie 24/05/13	24	l Dirección de Tecnología de la Información,Pc para Garitas [8]
26	Equipos de TV para circuito cerrado	5 días	lun 27/05/13	vie 31/05/13	25	enieria Civil y Portuaria,Equipos de TV para circuito cerrado[4]
27	**CIRCUITO CERRADO DE TELEVISIÓN**	**25 días**	**lun 03/06/13**	**vie 05/07/13**		
28	Instalación de Autodomos PTZs de 1/3 a color con Zoom de un mínimo de 28 X, blindajes y monturas para ser instalados en el exterior.	10 días	lun 03/06/13	vie 14/06/13	26	Personal de Dirección de Ingenieria Civil y Portuaria,Fiscalizadores,Personal de Seguridad Institucional de la Armada,Autodomos PTZs de 1/3 a color con Zoom de un mínimo de 28 X; blindajes y monturas para ser instalados en el exterior.[20]
29	Instalación de Cámaras a color con lente varifocal, autoiris, blindaje y montura para cubrir entrada y salida en la garita principal y el área operativa.	5 días	lun 17/06/13	vie 21/06/13	28	Personal de Dirección de Ingenieria Civil y Portuaria,Fiscalizadores,Personal de Seguridad Institucional de la Armada,cámaras a color con lente varifocal, autoiris, blindaje y montura para cubrir entrada y salida en la garita principal y el área operati.

	Nombre de tarea	Duración	Comienzo	Fin	ce	Nombres de los recursos
42	Instalación de Sirena de 30 W de altos decibeles con caja y tamper Switcher de protección por local	5 días	lun 27/05/13	vie 31/05/13	41	Fiscalizadores,Personal de Dirección de Ingenieria Civil y Portuaria,Personal de Seguridad Institucional de la Armada
43	**SISTEMA DE DETECCION PERIMETRICA**	**40 días**	**lun 03/06/13**	**vie 26/07/13**		
44	**PERIFON**	**20 días**	**lun 03/06/13**	**vie 28/06/13**		
45	Incluida mano de obra de instalación, programación y materiales	20 días	lun 03/06/13	vie 28/06/13	42	Fiscalizadores,Personal de Dirección de Ingenieria Civil y Portuaria,Personal de Seguridad Institucional de la Armada,vallas puerto[1]
46	**PERIGUARD**	**20 días**	**lun 01/07/13**	**vie 26/07/13**		
47	Incluida mano de obra de instalación, programación y materiales	20 días	lun 01/07/13	vie 26/07/13	45	Fiscalizadores,Personal de Dirección de Ingenieria Civil y Portuaria,Personal de Seguridad Institucional de la Armada,vallas fertiza[1]

Fuente: (León, 2012)

Autor: Ing. Cecibel León Arreaga



CAPITULO 5
Análisis y evaluación de costos

Para la implementación del proyecto es necesario incrementar hardware, software y equipos de seguridad física, los mismos que han sido mencionados en el capítulo anterior. En el presente capítulo se muestra cuáles son los costos, un flujo de caja tentativo y una comparación con las pérdidas que se tendría en caso de no incrementar el proyecto, y así poder determinar la factibilidad de su implementación

Flujo de caja

En el flujo de caja se han considerado todos los costos en que se incurriría para la elaboración del proyecto.

Flujo de caja

	CANT.	P.U.	SUBTOTAL	TOTAL
SEGURIDAD DE RED				
Cisco CS-MARS-200 Security Monitoring Analysis and Response System	1	22.000,00	22.000,00	
Router para VPN con varias conexiones WAN Cisco RV016 Cisco Small Business Routers	1	400,00	400,00	
Cisco ASA 5500 Series Model License Cisco ASA 5500 Series Modelo / licencia	1	7.500,00	7.500,00	29.900,00
CAMBIO DE SOFTWARE				
Cambios en Base de Datos (personal de DIGMAT)	1	0,00	0,00	
Cambios en Software (personal de DIGMAT)	1	0,00	0,00	
Servidor para almacenamiento de imágenes	1	2.000,00	2.000,00	
Servidor de contingencia para almacenamiento de imágenes	1	2.000,00	2.000,00	
Pc para Garitas	8	750,00	6.000,00	
Equipos de TV para circuito cerrado	4	1.500,00	6.000,00	$ 16.000,00
CIRCUITO CERRADO DE TELEVISIÓN				
Autodomos PTZs de 1/3 a color con Zoom de un mínimo de 28 X, blindajes y monturas para ser instalados en el exterior.	20	1.386,00	27.720,00	
cámaras a color con lente varifocal, autoiris, blindaje y montura para cubrir entrada y salida en la garita principal y el área operativa.	12	140,00	1.680,00	
Sistema de video grabación digital con disco duro de 1 terabyte y multiplexor de 16 canales de entrada.	2	2.600,00	5.200,00	
Sistema de video transmisión a través de fibra óptica.	19	50,00	950,00	
Instalación de 14 cámaras y cambio de sistema de control de video, configuración cableado electrico y datos, incluye cableado adicional de video, alimentación y conectores varios	2	300,00	600,00	36.150,00

	CANT.	P.U.	SUBTOTAL	TOTAL
SISTEMA DE CONTROL DE ACCESO				
Vallas eléctricas de 1/3 de H.P. cada uno, de alto rendimiento, con detector de presencia de vehiculo para evitar accidentes.	8	2.700,00	21.600,00	
torniquetes de control de ingreso y salida, leen tarjetas de aproximación	4	1.600,00	6.400,00	
Paneles de control de accesos con 8 lectoras de proximidad	4	250,00	1.000,00	
Instalación y software de acceso	1	0,00	0,00	
Tarjetas de proximidad	1000	7,00	7.000,00	$ 36.000,00
SISTEMA DE ALARMAS CONTRA ROBO, ASALTO				
Panel de control (se usaria el mismo de circuito cerrado)	1	0,00	0,00	
Sistema de alarma				
Detectores infrarrojos / microonda de movimiento de doble tecnologia, especial de alto	40	250,00	10.000,00	
Sirena de 30 W de altos decibeles con caja y tamper Switcher de protección por local				
Fuente de poder y bateria de respaldo por local				
Botonera de asalto				
Contactos magnéticos para puestas metálicas, por local	36	50,00	1.800,00	$ 11.800,00
SISTEMA DE DETECCION PERIMETRICA				
PERIFON	1	21.000,00	21.000,00	
Incluida mano de obra de instalación, programación y materiales				
PERIGUARD	1	36.000,00	36.000,00	$ 57.000,00
Incluida mano de obra de instalación, programación y materiales				
TOTAL DEL PROYECTO				**$ 186.850,00**

Premisas de proyección

A continuación la evaluación financiera del proyecto con el fin de determinar la factibilidad económica del presente proyecto para la Dirección General del Material.

Para realizar la evaluación financiera se realizó la recopilación de información fiable y necesaria.

Estas premisas son las siguientes:

1. Tasa de Inflación: 4.5%.
2. Años de Proyección: 5 años.

3. Método: Flujo de Caja Futuro Descontado.
4. Incremento en gastos ajustados a la tasa de Inflación.
5. Impuesto a la Renta: 0%.
6. Participación de Trabajadores: 0%.
7. Tasa de Descuento: 25%. Esta tasa es la tasa del costo de oportunidad del accionista.
8. No hay financiamiento por ende ni servicio de deuda.

A continuación, una pequeña inducción sobre algunos elementos importantes para el análisis económico y financiero.

El costo de oportunidad es el valor de los beneficios a los que se renuncia al escoger, según criterio propio, la mejor alternativa, y se da principalmente porque existen dos o más alternativas de inversión y esto permite elegir la opción más rentable.

La Tasa de Inflación refleja el aumento porcentual de los precios en un cierto período de tiempo.

Tasa de Descuento es una medida financiera que se aplica para la actualización de flujos de caja de un proyecto, en este caso para determinar el valor actual de un pago futuro.

> Es el impuesto que se grava sobre los ingresos o rentas, producto de actividades personales, comerciales, industriales, agrícolas, y en general actividades económicas y aún sobre ingresos gratuitos, percibidos durante un año, luego de descontar los costos y gastos incurridos para obtener o conservar dichas rentas, (Asamblea Nacional, Gobierno de la República del Ecuador, 2010)

La Participación de Trabajadores en el Ecuador es del 15%, pero no aplica por ser una empresa pública y por ende no se entregan utilidades a los empleados.

La Tasa Activa Referencial es igual al promedio ponderado semanal de las tasas de operaciones de crédito de entre 84 y 91 días, otorgadas por todos los bancos privados, al sector corporativo.

Como se explicó en las premisas de proyección, la evaluación se dará a 5 años, descontando una tasa de costo de oportunidad del 25% para la consideración de la implementación por parte del Alto Mando del Sector del Material de la Fuerza Naval.

Los indicadores que se utilizarán son el Valor Presente Neto (VAN), el cual mostrará en el presente el valor de los flujos de dinero de la empresa, utilizando una Tasa de Descuento; la Tasa Interna de Retorno (TIR) será otro indicador a utilizar, la cual representa la rentabilidad porcentual del proyecto considerando los flujos de dinero por año, para luego hacer la comparación de la misma frente a la Tasa de Descuento

Evaluación Económica Financiera

Evaluación Económica Financiera							
CONSIDERAR GASTOS DE PERSONAL							
Tasa de Descuento (WACC)	**25% TASA ACTIVA REFERENCIAL**						
	0	1	2	3	4	5	TOTAL
Inversión Inicial	(186,850.00)						
Total Inversión Inicial	(186,850.00)						
Valor de inmuebles a marzo de 2012	808,954.17						
Costo de Incendio y/o robo 10% del valor actual de Inmuebles		80,895.42	80,895.42	80,895.42	80,895.42	80,895.42	404,477.09
Costo Actual		80,895.42	80,895.42	80,895.42	80,895.42	80,895.42	404,477.09
(=) Margen Bruto		80,895.42	80,895.42	80,895.42	80,895.42	80,895.42	404,477.09
	Inflación		4.50%	4.50%	4.50%	4.50%	
Costos Propuestos							
Soporte Técnico y mantenimiento		10,000.00	10,435.00	10,888.92	11,362.59	11,856.86	54,543.38
Costo entrenamiento (esta incluido en el soporte técnico)		0.00	0.00	0.00	0.00	0.00	0.00
Depreciación		37,370.00	37,370.00	37,370.00	37,370.00	37,370.00	186,850.00
(=) Total Costos Propuestos		47,370.00	47,805.00	48,258.92	48,732.59	49,226.86	241,393.38
(=) Margen Bruto		33,525.42	33,090.42	32,636.49	32,162.83	31,668.55	163,083.71
- 25% I.R.		0.00	0.00	0.00	0.00	0.00	0.00
-15% P.L.		0.00	0.00	0.00	0.00	0.00	0.00
Margen Neto		33,525.42	33,090.42	32,636.49	32,162.83	31,668.55	163,083.71
+ Depreciación		37,370.00	37,370.00	37,370.00	37,370.00	37,370.00	186,850.00
Flujo de efectivo Actualizado	(186,850.00)	70,895.42	70,460.42	70,006.49	69,532.83	69,038.55	
Valor Actual Flujo de Efectivo	186,850.00	115,954.58	45,494.17	(24,512.33)			

Autor: Ing. Cecibel León Arreaga.

CALCULO E INTERPRETACIÓN DEL VALOR ACTUAL NETO (VAN)

La técnica del Valor Actual Neto (VAN) o Valor presente Neto (VPN) es la que se utiliza con mayor frecuencia para tomar decisiones de inversión en activos fijos, conceptualmente es la diferencia entre el valor actual de los flujos netos de caja estimados del proyecto y la inversión neta requerida.

El Valor Actual Neto es la cantidad monetaria que resulta de convertir los flujos de valores de ingresos y gastos futuros hacia el presente; utilizando una tasa de descuento. De esta manera, la técnica del VAN permite identificar el ingreso neto futuro en función de la pérdida de poder de compra de dichos ingresos, utilizando una tasa de interés específica.

El valor actual neto es un indicador sencillo de llevar a la práctica y que nos ayuda a realizar un análisis confiable ya que tiene en cuenta el valor del dinero en cada momento. Además, es muy flexible ya que permite introducir en el criterio cualquier variable que pueda afectar a la inversión, inflación, etc.

El VAN ofrece un valor fácilmente comprensible y los criterios de decisión de inversiones son los siguientes:

Criterios de Inversión

Resultado	Interpretación
VAN = 0	Los ingresos son iguales a los costos. No se pierde ni se gana. No se recomienda invertir pero algunos analistas recomiendan realizar la inversión.
VAN > 0	Los ingresos son mayores que los costos. Se obtendrán ganancias, por tanto, se recomienda realizar la inversión.
VAN < 0	Los ingresos son menores que los costos. Se obtendrán pérdidas, por tanto, no se recomienda realizar la inversión.

El proyecto se acepta siempre y cuando el VAN sea mayor o igual a cero, caso contrario se rechaza.

El mayor problema para aplicar este método radica en fijar la tasa correcta de descuento (costo de capital), ya que es la variable más influyente para saber si el proyecto será o no rentable.

Indicador	Valor
Inversión neta	USD 186,850
Sumatoria Flujos de caja	USD 163,084
VAN	USD 1,526

De acuerdo al criterio de evaluación derivado de la aplicación de la técnica del valor actual neto, el proyecto de Seguridad de Base Naval Sur es viable, el VAN es mayor que cero y positivo. Es decir el proyecto genera un rendimiento mayor que el costo de los recursos externos de financiamiento y por lo tanto, desde este punto de análisis, conviene ejecutar el proyecto.

CÁLCULO E INTERPRETACIÓN DE LA TASA INTERNA DE RETORNO (TIR)

La Tasa Interna de Retorno es la tasa de descuento que hace que el valor presente neto de la inversión igual sea cero, es decir que el valor presente de los flujos de caja que genera el proyecto sea exactamente igual a la inversión neta realizada.

La tasa interna de retorno (TIR), es aquella tasa de interés que representa la rentabilidad porcentual del proyecto, considerando un flujo de beneficios netos por año, para luego hacer la comparación frente a la Tasa de Descuento.

La TIR es la tasa de interés más alta que se podría pagar sin perder dinero, si todos los fondos para el financiamiento de la inversión se tomaran prestados, y éste se pagará con las entradas de efectivo de la inversión, a medida que el proyecto avanza en su vida útil.

El criterio de selección utilizando la TIR se basa en la aceptación de todas las inversiones cuya TIR sea mayor que el costo de oportunidad. Y ya que el cálculo manual de este indicador es complicado porque debe realizarse mediante aproximaciones sucesivas, se recomienda la utilización de hojas electrónicas que ya traen incorporados los comandos para realizar el cálculo rápido utilizando los ingresos netos.

El criterio para aceptar o rechazar el proyecto se fundamenta en que si la TIR es menor que la tasa de descuento se debe rechazar el proyecto, en caso contrario se lo acepta.

Indicador	Valor
TIR	25%

En relación al cuadro anterior de la Tasa Interna de retorno derivada de la alternativa presentada de composición de capital para la inversión, se concluye lo siguiente:

Que la tasa de retorno obtenida en el proyecto de seguridad física computarizada de DIGMAT es superior al costo de los recursos de financiamiento externo, por lo tanto, el proyecto puede soportar un incremento en la tasa de interés por tener margen de retorno de la inversión.

CÁLCULO E INTERPRETACIÓN DEL PERíODO REAL DE RECUPERACIÓN O PAYBACK (PRR)

El plazo real de recuperación de la inversión o payback (PRR), es el tiempo que tarda exactamente en ser recuperada la inversión inicial, en base a los flujos netos de caja actualizados que genere el proyecto, en este caso, durante su vida útil.

Inversión neta	**USD 186,850**	
Año	**Flujos Netos de Caja Descontados**	**Recuperación de la Inversión Neta**

1	$70,895.42	-$115,954.58
2	$70,460.42	-$45,494.17
3	$70,006.49	$24,512.33
4	$69,532.83	$94,045.15
5	$69,038.55	$163,083.71

Indicador	Valor
PRR	**3**

Este es un criterio de liquidez antes que de rentabilidad; va a permitir tomar decisiones en situaciones de riesgo. En relación al cálculo realizado, se obtuvo un período real de recuperación equivalente a 3 años.

CONCLUSIONES

Luego de un adecuado análisis se puede deducir que los problemas actuales encontrados son los siguientes:

En la actualidad la Fuerza Naval cuenta con un nivel de seguridad bajo, muchos de los controles de seguridad son manuales, como llevar las bitácoras manuales de ingreso y salida de los visitantes.

La necesidad de un sistema informático que permita llevar el control de los vehículos y personas que ingresen a la Base Sur es totalmente evidente.

Los sistemas con que se cuenta son para el registro de la asistencia del personal, especialmente la tropa y personal de servidores

Las zonas que colindan o limitan la base Naval sur con la población civil

Los puntos mencionados anteriormente mejorarán al implementar un sistema de seguridad, tanto de acceso físico como a los aplicativos, totalmente automatizado y que brinde las facilidades de cambio de los accesos a los sistemas.

Lograr que los usuarios no tengan que solicitar cambios cada vez que cambian de plaza (lugar de trabajo), que no tengan que pedir permisos para cada área sino que por su rango y funciones dentro de la institución tengan automáticamente los permisos. Y que los usuarios externos se vean obligados a ingresar sus datos en bitácora electrónica para tener un registro de quien ingresa y sale del edificio

Al mejorar los aspectos mencionados, se logrará el cumplimiento de los objetivos establecidos en el presente trabajo tales como un Sistema de Seguridad 100% automatizado, a la vanguardia en el Ecuador que permita el control del acceso a las diferentes áreas del edificio de la Dirección General del Material en un plazo máximo de 1 año.

Lograr que el personal este 100% capacitado sobre el reglamento de seguridad de la institución en un plazo de 2 años como máximo.

La inversión a realizarse es de $ USD 186,850, un costo aparentemente elevado, pero si se contemplan los logros de tener una base con la seguridad física necesaria, bastaría para determinar que el proyecto debe ser llevado a cabo, pero si además se compara las posibles péerdidas, solo poniendo el 10% del valor del activo por año, resulta lo suficientemente rentable, lo cual es verificable al observar que el Valor Actual Neto (VAN) es de USD 1,526 y tasa interna de retorno es del 25% aproximadamente.

RECOMENDACIONES

Se recomienda implementar el sistema automatIzado de seguridad física en el Edificio DIGMAT/DIGREH. Para que la implementación del sistema sea un éxito deben considerarse los siguientes aspectos:

1. Capacitar a las personas involucradas directamente e indirectamente en la seguridad física; en especial al personal que será encargado de las cámaras de vigilancia. Pero sobre todo de la importancia de contar con los datos reales de quienes ingresan y salen de la Base naval sur, y que ingresen a la DIGMAT.

2. Periódicamente realizar controles del uso del sistema, para conocer la capacidad de conocimientos del uso del mismo, tanto del manejo informático como de la seriedad que se esté dando en los procedimientos.

3. Al mejorar todos los procedimientos del ingreso y salida de la base y del edificio DIGMAT, se evitarán problemas; además de mejorar la imagen de la institución puesto que por ser una institución militar debe tener un alto nivel de seguridad.

El uso de los sistemas informáticos automatizados es algo que se debe aplicar en toda institución como la DIGMAT, pues la fuga de información representa un alto riesgo.

BIBLIOGRAFÍA

Abastecimientos Secretaría de la Dirección de Organigrama de la Dirección de Abastecimientos. - Guayaquil : [s.n.], 20 de Enero de 2010.

Ambrosio Vicente Plan de Marketing paso a paso - Vicente Ambrosio . - México : [s.n.], 1978.

Asamblea Nacional, Gobierno de la República del Ecuador REGLAMENTO DE APLICACIÓN DE LA LEY DE RÉGIMEN TRIBUTARIO INTERNO. - 2010.

CERTO Samuel y PETER Paul Mejoramiento de los Procesos de la Empresa [Libro]. - Bogota : McGraw Hill/Interamericana, 1997.

CETEIN DIGMAT Manual del Sistema de Vigilancia. - Guayaquil : [s.n.], 2008.

CETEIN-DIGMAT Centro de tecnologia de la información DIGMAT Manual de Usuarios de Sistema de Seguridad. - Guayaquil : [s.n.], 2008.

CETEIN-DIGMAT Manual de lector de huella digital. - Guayaquil : [s.n.], 2010.

CETEIN-DIGMAT y León Ing. Cecibel Trabajo en grupo con Analista de CETEIN-DIGMAT // Diseño del Modelo Entidad- Relación en Base a los nuevos Procesos . - Guayaquil : [s.n.], 2012.

CISCO CISCO [En línea]. - 15 de 12 de 2012. - www.cisco.com.

Colamarco Rafaela y León Ing. Cecibel Analista de Procesos de la DIGMAT // Grupo de trabajo para definir lso nuevos procesos. - Guayaquil : [s.n.], 01 de 2013.

DIGMAT Departamento de Normalización y Seguridad Proyecto de Seguridad Física de BASUIL. - Guayaquil : [s.n.], 2003.

DIGMAT Departamento de Procesos de la Estatuto Orgánico de la Dirección General del Material. - Guayaquil : [s.n.], 2008.

DIRITC Dirección de Tecnología de la Información Diseños de redes de la Armada del ECuador. - Guayaquil : [s.n.], 2012.

DIRTIC Direccion de Tecnología de la información Armada del Ecuador [En línea]. - DIRTIC, 1 de 01 de 2013. - 15 de 01 de 2013. - http://www.armada.mil.ec/mision-y-vision;jsessionid=2293E5ECA9C1FFB5296E3BA42D049529.

DIRTIC Dirección de Tecnología de la Información Armada del Ecuador [En línea]. - 1 de 12 de 2012. - 15 de 03 de 2013. - http://www.armada.mil.ec/historia.

DIRTIC Direccion de técnologias de la Información Proyecto de implementación de seguridad física en DIRTIC. - Guayaquil : [s.n.], 2005.

ESPINOZA PEDRO VARGAS DISEÑO E IMPLEMENTACIÓN DE INDICADORES DE GESTION BAJO LA METODOLOGIA DEL BALANCED SCORECARD (CUADRO DE MANDO INTEGRAL) PARA EL PROCESO DE ABASTECIMIENTO DE BIENES Y SERVICIOS EN EL SECTOR PUBLICO. - Guayaquil : TESIS DE GRADO, ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL (ESPOL), 2008.

Fred David Conceptos de Administracion Estrategica [Sección de libro]. - Mexico : Prentice Hall Hispano Americano, 1997.

Fred R. David Conceptos de administración estratégica [Sección de libro]. - México : Prentice Hall Hispano Americano, 1997.

Información Dirección de Tecnologias de la y León Ing. Cecibel Diseño de la Red de la Armada en Base a Medidas de Seguridad // Diseño de la Red de la Armada en Base a Medidas de Seguridad. - Guayaquil : [s.n.], 2013.

Investigación del proceso Actual Investigación del proceso actual. - Guayaquil : [s.n.], 2012.

León Ing. Cecibel Diseño Pantallas realizado en base a Nuevos Procesos // Diseño Pantallas realizado en base a Nuevos Procesos. - Guayaquil : [s.n.], 2012.
León Ing. Cecibel Investigación de precios en internet y en empresas de Guayaquil. - Guayaquil : [s.n.], 2012.
León Ing. Cecibel Resultado de Investigación de costos en internet y proformas . - Guayaquil : [s.n.], 2012.
Only Control S.A. Manual de Usuario del Sistema Biométrico. - Guayaquil : [s.n.], 2010.
ONLYCONTROL DICCIONARIO DE DATOS - MODELO ENTIDAD RELACION. - Guayaquil : [s.n.], 2010.
Roe David http://www.cmswire.com/ [En línea] // http://www.cmswire.com/. - 13 de Mayo de 2011. - http://www.cmswire.com/cms/enterprise-collaboration/are-productivity-alternatives-hitting-microsoft-office-upgrades-011226.php.
Salazar Hernando Zabala Planeacion estrategica aplicada a cooperativas y demas formas asociativas y solidarias [Sección de libro]. - Colombia : [s.n.], 2005.

SOBRE LOS AUTORES

Cecibel León Arreaga

Es docente del área de Desarrollo de Sistemas en la Carrera de Ingeniería en Sistemas Administrativos Computarizados de la Universidad de Guayaquil. Ha realizado labores de docencia en la Universidad Estatal del Milagro en el año 2005, catedra en sistemas de información en el Tecnológico Naval Nocturno de 2002-2008

Realizo sus estudios universitarios en la Universidad de Guayaquil, obteniendo los títulos de Master en Administración de Empresas con Mención en Sistemas de Información Empresarial en la Facultad de Administración. En la Facultad de Ingeniería Industrial obtuvo los títulos de Ingeniera Industrial, y master en Seguridad, higiene Industrial y Salud Ocupacional, y el titulo de Analista de Sistemas en la Escuela Superior Politécnica del Litoral.

Posee una gran experiencia relacionada análisis y diseño de Sistemas de Información, en el Banco del Pacífico, La empresa Municipal de Agua Potable de Guayaquil - ECAPAG, la Escuela Superior Politécnica del Litoral, la Armada del Ecuador como Analista de Tecnologías de Información, actualmente realiza actividades de Técnico de Seguridad y Salud Ocupacional en la Armada del Ecuador.

Jorge Misael Merchán Riera

Es docente del área de Desarrollo de Sistemas en la Carrera de Ingeniería en Sistemas Administrativos Computarizados de la Universidad de Guayaquil.

Ha participado en proyectos de Diseño Curricular en la Universidad de Guayaquil y Proyectos de Investigación así como también ha escrito artículos científicos Orientados a la implementación de Tecnología.

Realizó sus estudios universitarios en la Universidad Católica de Santiago de Guayaquil, en donde obtuvo el título de Ingeniero en Sistemas Computacionales, cursó un Posgrado en la Escuela de Organización Industrial de Madrid España donde obtuvo el título de Master en Gestión de las Telecomunicaciones y Tecnologías de la Información, y también cursó un Posgrado en la Universidad de Guayaquil donde obtuvo el título de Magister en Educación Superior.

Adicionalmente ha realizado Certificaciones Profesionales como Desarrollador de Software en Java y Oracle y cuenta también con la certificación PMP la cual es una de las más reconocidas a nivel mundial en lo referente a gestión de Proyecto.

Posee una gran experiencia relacionada a la implementación de Sistemas de Información, ha participado dirigiendo muchos proyectos en empresas de múltiples sectores tanto públicas como privadas y ha ocupado puestos de Dirección en empresas tecnológicas.

Patricia Marcillo Sánchez

Nacido en 1978 en Guayaquil, Profesional en el area de Sistemas de Informacion y Administración, Licenciada en Sistemas de Información y Analista de Sistemas en Escuela Politecnica del Litoral(ESPOL).
Master en Administración de Empresas con Mención en Sistemas de Información Empresarial en la Facultad de Administración de la Universidad de Guayaquil.
Maestrante de la Universidad Politécnica de Madrid España (UPM), Máster Universitario en Ciencias y Tecnologías de la Computación
Experiencia Laboral
2016- Actual Docente en la Universidad de Guayaquil en la Facultad Ciencias Administrativas en la carrera de Ingeniería en Sistemas Administrativos Computarizados de la Universidad de Guayaquil, en área de desarrollo de Sistemas. 2014-2015 en la Universidad Politécnica Salesiana Guayaquil en el área de Sistemas en la Facultad de Sistemas. 2014-2015 en la Universidad de Guayaquil en la Facultad de Matemáticas en el área de Sistemas. 2013-2015 en el Tecnológico Superior Provincia de Tungurahua en carrera de Analista de Sistemas.
Laboró en la ARMADA DEL ECUADOR por 14 años 2000-2014 en departamento de Sistemas de Dirección General del Material como Analista de Tecnología de la Información, desempeño las labores de: Análisis, desarrollo e implementación de Sistemas Administrativos Financieros y Sistemas de Control de Obras , Capacitación de Usuarios, Levantamiento de Procesos.
Asesora y Desarrolladora Independiente de Sistemas Administrativos Financieros para Empresas.

Johanna Zumba Gamboa

Es docente del área de Desarrollo de Sistemas y Gestora del Criterio Plan Curricular en la Carrera de Ingeniería en Sistemas Administrativos Computarizados de la Universidad de Guayaquil.
Su trabajo de Investigación está enfocado en el área Tecnología de Información y Comunicación en Educación, publicando su primer artículo científico en la revista Eduweb.
Realizo sus estudios universitarios en la Universidad de Guayaquil, recibió su maestría en Administración de Empresas con Mención en Sistemas de Información Empresarial en la Facultad de Administración y la Ingeniería en Sistemas Computacionales en la Facultad de Ciencias Matemáticas y Físicas.
Posee una gran experiencia relacionada análisis y diseño de Sistemas de Información, antes de ejercer la docencia trabajó en la ARMADA DEL ECUADOR como Analista de Tecnologías de Información, actualmente realiza actividades de consultoría externa para la empresa InnovaSystem Ecuador S.A, entidad dedicada a la consultoría e implementación de soluciones de negocio basada en tecnología.

LA SEGURIDAD FÍSICA AUTOMATIZADA EN LA ARMADA DEL ECUADOR

PRIMERA EDICIÓN

ISBN: 978-9942-760-50-0