ESCUELA POLITÉCNICA DEL EJÉRCITO

FACULTAD DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

DESARROLLO DEL MANUAL DE SEGURIDADES INFORMÁTICAS DE LA ARMADA DEL ECUADOR

Previa a la obtención del Título de:

INGENIERO DE SISTEMAS E INFORMÁTICA

POR: MÓNICA ALEXANDRA LLERENA FUENMAYOR
JOSÉ DAVID SAÁ CHONLONG

SANGOLQUÍ, 20 DE ABRIL DEL 2006

CERTIFICADO

Certifico que el presente trabajo fue realizado en su totalidad por los Srs. Mónica Alexandra Llerena Fuenmayor y José David Saá Chonlong, como requerimiento parcial a la obtención del título de INGENIERO DE SISTEMAS E INFORMÁTICA.

Fecha: 20 de Abril del 2006

Ing. Diego Marcillo
Director de Tesis

DEDICATORIA

Dedicamos este trabajo a nuestros padres que con su esfuerzo nos apoyaron en el transcurso de nuestra carrera, así como, han sido guía y ejemplo de responsabilidad para cumplir nuestros objetivos. Y a nuestros hermanos por acompañarnos en todo momento y poner su confianza en nosotros.

Mónica Llerena Fuenmayor

José David Saá Chonlong

AGRADECIMIENTOS

Agradecemos infinitamente a Dios por habernos dado la vida y salud para vencer cualquier dificultad, así como la oportunidad de seguir una carrera, a nuestros padres por brindarnos su confianza, cariño y apoyo, a nuestros hermanos y amigos por acompañarnos en todo momento, a nuestros maestros que colaboraron en nuestra formación profesional y a todos quienes hicieron posible para el cumplimiento de este trabajo.

Mónica Llerena Fuenmayor

José David Saá Chonlong

ÍNDICE

Listado de Tablas

Listado de Cuadros

Listado de Figuras

Listado de Anexos

Nomenclatura utilizada

Sigla	Descripción
568A, 568B	Estándar de cableado estructurado
BIOS	Basic Input/Output System
CETEIQ	Centro De Tecnología De La Información Quito
CETEIG	Centro De Tecnología De La Información Guayaquil
COGMAR	Comandancia General de Marina
COOPNAPRIZON	Comando de Operaciones Navales y Primera Zona Naval
CP	Valor de los bienes y recursos protegidos
CPD	Administración de Centro de Cómputos
DIGAFI	Dirección General Administración Financiera
DIRDAI	Dirección de Desarrollo Administrativo e Informático

DIGEIM	Dirección General de Intereses Marítimos
DIGEDU	Dirección General de Educación
DIREMP	Dirección de Empresas
DIRINT	Dirección de Inteligencia
DIRFIN	Dirección Finanzas
DIGMAT	Dirección General del Material
DIGMER	Dirección General de la Marina Mercante y del Litoral
DIGPER	Dirección General del Personal
DNS	Domain Name Server
DoS	Disk Operating System
ESMAAR	Estado Mayor de la Armada
FTP	File Transfer Protocol
ID	Identificación
Ids	Sistema de detección de intrusos
INSGAR	Inspectoría General de la Armada
IP	Internet Protocol
ISO	Internacional Standard Organization
IT	Information Technology
KPBS	KiloBytes Per Second
LAN	Red de Área Local
MSN	Messenger
PC	Personal Computer
SQL	Structured Query Language
UPS	Uninterruptible power supply
UTP	Unshielded Twisted Pair
WAN	Red de Área Extendida

Resumen

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse “a medida”, para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes. De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

Por esta razón, en el presente trabajo final se elaboró un Manual de Seguridades Informáticas para la Armada del Ecuador, lo que implica que, por ser una Institución

militar se necesita de una concientización y planteamiento de políticas que salvaguarden la confidencialidad de sus activos informáticos, verificando así la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y el cumplimiento de los reglamentos y normas prescriptas.

Como resultado se realiza un análisis de la situación actual de su entorno informático permitiendo determinar el nivel de riesgos que enfrentan sus activos y a que factores se encuentran expuestos, para así generar políticas enmarcadas dentro de las normas Institucionales y principalmente tratando de conseguir la confidencialidad, integridad, disponibilidad, autenticidad y no-repudiación de sus datos.

Capítulo 1. Introducción

1.1.- Introducción

A medida que la tecnología ha ido evolucionando y con ella, la envergadura de los sistemas de información de las instituciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, información, etc.) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los directivos, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución.

En la actualidad, las inversiones en seguridad que realizan las empresas se están destinando cada vez menos exclusivamente a la compra de productos, y comienzan a destinar parte de su presupuesto a la gestión de la seguridad de la información. El concepto de seguridad ha variado, asegurándose un nuevo concepto, el de seguridad gestionada, que ha suplantado al de “seguridad informática”. Las medidas que comienzan a tomar las empresas giran entorno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes: técnica, legal y organizativa, es decir, un planteamiento coherente de directrices, procedimientos y criterios que permiten desde la dirección de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de Información, la organización afín y sus infraestructuras.

La Gestión de la Seguridad de la Información (SI) en una organización se consigue mediante planificación, análisis de activos y de riesgos, selección de controles técnicos, así como, su difusión, formación y aplicación. La seguridad de la información implica tanto a la información que está basada en sistemas informáticos o en papel, como a las personas.

La información es el patrimonio principal de toda organización, y más aún dentro de una Institución Militar como es la Armada del Ecuador. Como enuncian sus políticas y su arquitectura tecnológica actual, existe la necesidad de implementar seguridades informáticas, que mediante la orientación de la Dirección de Desarrollo Administrativo e Informático se identificará la situación actual de la Institución tanto en sus activos informáticos como de comunicación de datos, las medidas de seguridad para protegerlos y la visión proactiva para afrontar contingencias y desastres de diversos tipos.

Es relevante mencionar que el proyecto tesis generará una propuesta de un Manual de Seguridades Informáticas basado en los lineamientos generales sobre Seguridad Informática citados en la Norma ISO 17799:2000 que para el inicio del estudio actual era la Norma vigente. Si en el futuro se requiere el desarrollo e implementación definitiva de un Manual de Seguridad Informáticas se deberá basarse en los lineamientos generales sobre Seguridad Informática citados en la Norma ISO 17799:2005 y en la especificación de controles de la Norma ISO 27001.

La Seguridad de la Información hoy día no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología. Al identificar dichos recursos se podrá alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. Además sino se cuenta con reglas, lineamientos, responsabilidades y procedimientos predefinidos, y ante la ausencia de personal que es capacitado para la gestión del proceso, la inversión en tecnología no es más que una pérdida de dinero. Este concepto de Seguridad de la Información como una solución integral es esencial para la transformación de este nuevo enfoque, en una plataforma

tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para el negocio. En este sentido, la Seguridad de la Información es un aspecto sumamente importante en la relación que se establece entre el negocio, sus clientes, socios, proveedores y empleados.

1.2.- Objetivos

1.2.1.- Objetivo General

Desarrollar una propuesta de un Manual de Seguridades Informáticas para la Armada del Ecuador a fin de alcanzar la eficiencia y eficacia en las actividades de resguardo o protección de los activos informáticos.

1.2.2.- Objetivos Específicos

- Determinar la situación actual de la Seguridades Informática y de Comunicaciones de datos de la Dirección de Desarrollo Administrativo e Informático de la Armada del Ecuador.

- Identificar las áreas de la Arquitectura de Seguridad (Lógica, Física, Aplicaciones y Comunicaciones) y con ello elaborar las políticas respectivas para cada área.

- Elaborar la propuesta del Manual de Seguridad Informática según la estructura y formato específico de la Armada del Ecuador.

1.3.- Planteamiento del Problema

Teniendo en cuenta el gran avance tecnológico que forma nuevas condiciones y plataformas informáticas, surge la aparición de nuevas amenazas en los sistemas informáticos, teniendo el riesgo de que la información no sea utilizada adecuadamente, es decir, en perjuicio de la Institución por lo que se ha convertido en una de las grandes

preocupaciones de las Organizaciones. Esta preocupación debe ser adecuadamente comprendida y compartida por todos los que conforman la empresa y más por los directivos los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución

1.4.- Justificación

Por este motivo la importancia de resguardarla y limitarla, poniéndola a disposición únicamente del personal con una real necesidad. Bajo estas consideraciones, el propósito del Desarrollo de un Manual de Seguridades Informáticas es: Proteger los activos informáticos, contra amenazas que pueden ser internas o externas; identificar los riesgos a los que se encuentra expuesta la información de la Armada; diseñar correctivos apropiados basados en políticas y estándares de seguridad que colaboren a reducir el riesgo a un nivel aceptable; utilizar a las políticas de Seguridad Informática como una herramienta para concienciar a los miembros de la Institución sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la Institución desarrollarse y mantenerse en su sector de trabajo.

1.5.- Alcance

Siendo la Seguridad Informática parte de la Seguridad de la Información el presente proyecto de tesis está orientado a proponer un Manual de Seguridades Informáticas para la Armada del Ecuador basado en los lineamientos de la Norma ISO 17799:2000 (se utilizaron los dominios de Seguridad Organizacional, Clasificación y control de Activos, Seguridad del Personal, Seguridad Física y Ambiental, Gestión de Comunicaciones y Operaciones y Control Acceso) así como los lineamientos de la Institución. Para la realización del análisis de la Situación Actual de Seguridades Informáticas de la Institución

se aplicaron los cuestionarios al Departamento de Desarrollo Administrativo e Informático (DIRDAI), ya que este es el encargado de dar soporte técnico y administrativo en el área informática a la Armada del Ecuador.

1.6.- Metodología

En el proyecto de tesis se realizó los siguientes pasos:

- **Fase I: Determinar la situación actual.-** En esta fase se realizó el análisis de riesgos, identificando los riesgos que se enfrentan los activos computacionales y comunicación de datos, así como la identificación y su nivel de importancia de los activos y riesgos, para obtener el nivel de vulnerabilidad de cada activo.
- **Fase II: Diseño de la Arquitectura de Seguridad.-** Se analizó los resultados obtenidos de la fase anterior, y con ello se identificó las áreas de la Arquitectura de la Seguridad Informática (área lógica, área física, área de aplicaciones y áreas de comunicaciones) y con ellas se realizó el diseño de controles adecuados basados en los lineamientos de la Norma ISO 17799:2000.
- **Fase III: Elaboración del Manual de Seguridad.-** En esta fase se realizó la propuesta del Manual de Seguridades Informáticas, su estructura y formato se basó en la Guía de Manuales de la Armada del Ecuador.

Capítulo 2. Marco Teórico

2.1.- Seguridad Informática

2.1.1.- Definición de Seguridad Informática

Cuando se habla de la función de la informática generalmente se tiende a hablar de nuevas tecnologías, de nuevas aplicaciones, nuevos dispositivos de hardware nuevas formas de elaborar información más consistente. La base para la existencia de los elementos anteriores es la información.

La información es un activo importante que tiene valor para una organización y en consecuencia necesita ser protegido adecuadamente, la información puede existir en muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente transmitida por correo o utilizando medios electrónicos o hablada en conversaciones. Cualquiera que sea la forma que tome la información, o el medio por el cual se comparten o se almacena, siempre se debe protegerla apropiadamente.[1]

No existe una definición estricta de lo que se entiende por seguridad informática, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los Sistemas de Información, áreas que van desde la protección física hasta la protección lógica, diversos tipos de amenazas contra los que debemos protegernos p.e. amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos, el robo, destrucción o modificación de la información.

Por lo tanto, la Seguridad informática se debe entender como, la interrelación de diferentes etapas, que al final del proceso garanticen elementos esenciales al interior de

[1] Norma ISO/IEC 17799

sus sistemas como son: confidencialidad, disponibilidad e integridad de la información[2]. Dependiendo del tipo de sistema informático con el que tratemos (militar, comercial, bancario), el orden de importancia de estos tres factores es diferente, e incluso entran en juego otros elementos como la autenticidad o el no repudio. [3]

2.1.2.- Importancia de la Seguridad Informática

La información y los procesos son activos comerciales importantes, la confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener una ventaja competitiva, rentabilidad, conformidad legal e imagen comercial.

La seguridad Informática se logra implementando un conjunto de controles adecuados; que podrían ser políticas, procedimientos, estructuras organizacionales y funciones de software. Se necesita estos controles para asegurar que se cumplan los objetivos de seguridad específicos de la organización.

Cada vez más las organizaciones y sus sistemas se enfrentan a amenazas contra su seguridad desde un rango amplio de fuentes; incluyendo fraude por medio de computadoras, espionaje, sabotaje, vandalismo, virus informático, incendio o inundaciones.

La dependencia en los sistemas y servicios de información significa que las organizaciones son más vulnerables a las amenazas a la seguridad. Muchos sistemas de información no han sido diseñados para ser seguros, la seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser respaldada por una gestión y

[2] http://people.fluidsignal.com
[3] www.softdownload.com.ar

procedimientos apropiados.[4] El punto de partida para un sistema de seguridad informática es la realización del diagnóstico de la situación actual, para luego poder proyectar las soluciones necesarias a cada caso mediante políticas de seguridad.

2.1.3.- Variables de la Seguridad Informática

2.1.3.1.- Confidencialidad

La confidencialidad, a veces denominada privacidad, es la necesidad de que la información sólo sea conocida por personas autorizadas, asegura que la información no pueda estar disponible por o para otras personas, entidades o procesos no autorizados. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño o volverse obsoleta.

En áreas de seguridad gubernamentales el secreto asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo[5]:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

[4] Norma ISO/IEC 17799
[5] www.softdownload.com.ar

2.1.3.2.- Integridad

La integridad garantiza que la información debe ser modificada creada y borrada sólo por el personal autorizado y dicha modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

Esta propiedad permite asegurar que no se ha falseado la información, el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados.

2.1.3.3.- Disponibilidad

La disponibilidad u operatividad es la capacidad de la información al estar en el lugar, momento y forma en que es requerido por el usuario autorizado para ser procesada en un periodo de tiempo aceptable. Esto requiere que la misma se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente respetando los formatos para su recuperación satisfactoria en caso de fallo.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*).

Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados.

2.1.3.4.- Autenticidad

La autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades[6].

2.1.3.5.- No-repudio

Dentro de un sistema de información la característica del no-repudio permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

2.2.- Requerimientos de Seguridad

2.2.1.- Análisis de Riesgos

2.2.1.1.- Definición

El análisis de riesgos es una actividad esencial que implica la evaluación de las actividades de la organización en base al análisis de activos, amenazas, vulnerabilidades, riesgos e impactos.

La identificación de los requerimientos de seguridad permite determinar cuáles de los activos de la empresa tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, considerando el grado en que el riesgo puede ser controlado y definiendo los servicios y las medidas de seguridad que se deben implementar para proteger un determinado entorno de la organización.

[6] http://www.segu-info.com.ar

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

2.2.1.2.- Pasos para el análisis de riesgo

2.2.1.2.1.- Lista de activos

Para listar los activos de información se debe evaluarlos en criterios de hardware, software y de datos pertenecientes a la organización, generando un inventario de aquellos que son considerados como vitales para su desenvolvimiento seguro.

Dentro de los activos de información podemos citar a[7]:

- **Hardware**: servidores, estaciones cliente, dispositivos de comunicación (router, bridge, hub, gateway, modem), dispositivos periférico, cables, fibras, etc.
- **Software (o Servicios):** Sistemas operativos de red, sistemas operativos en estaciones cliente, aplicaciones, herramientas (administrativas, mantenimiento, backup), software bajo desarrollo.
- **Datos:**
  - De la organización: bases de datos, hojas electrónicas, procesamiento de palabra, e-mail.
  - De la red: Privilegios de acceso a usuarios, password de usuarios, pistas de auditoria, configuración y parámetros de la red.
  - De los usuarios: datos procesados personal, archivos de propiedad del usuario.

[7] Taller Administración de Riesgos Bogotá, D.C. Octubre 8 de 2003

2.2.1.2.2.- Asignación de prioridades a los activos

Una vez que se identifican los activos de información se los debe clasificar según el impacto que sufriría la organización si faltase o fallara tal activo, para ello se les asignará un valor a la importancia que tienen en la Institución, ponderada en una escala del 1 al 10. Esta importancia es un valor subjetivo que refleja el nivel de impacto que puede tener la empresa si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

2.2.1.2.3.- Factores de riesgo

Acto seguido se debe listar los factores de riesgo relevantes a los que pueden verse sometidos cada uno de los activos identificados anteriormente. Determinando su nivel de probabilidad de que estas contingencias ocurran, en una escala del 1 al 3 o también en una ponderación de Bajo-Medio-Alto. Esta probabilidad será evaluada y determinada teniendo en cuenta las medidas de seguridad existentes en la Institución.

2.2.1.2.3.1.- Tipos de riesgos

Es importante de destacar que los riesgos que a continuación se especificarán son una generalización de todos los tipos de riesgos que pueden existir.

De los cuales se detalla a continuación:

Sabotaje Informático.- El Sabotaje informático, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Fraude.- Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. Las tres principales áreas donde se produce el fraude son:

1. Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples y, en general, conocidos por un gran número de personas de la empresa.
2. Alteración o creación de archivos de información. Se alteran los datos directamente del fichero o se modifica algún programa para que realice la operación deseada.
3. Transmisión ilegal. Interceptar o transferir información de teleproceso.

Robo.- Apoderarse de una cosa ajena de cualquier modo que sea tomada. Los equipos de cómputo son posesiones muy valiosas de las empresas y están expuestas al robo. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraída, cintas y discos son fácilmente copiados sin dejar ningún rastro.

Catástrofe climática.- Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la

existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Incendios.- El fuego es un elemento comprendido dentro de las principales amenazas contra la seguridad. El fuego es un problema crítico en un centro de cómputo por varias razones: primero, porque el centro está lleno de material combustible como papel, cajas, etc. El hardware y el cableado del suelo falso pueden ser también fuente de serios incendios. Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

Inundaciones.- Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Virus informático.- Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

2.2.1.2.4.- Consecuencias Y Medidas Existentes

Teniendo presente el listado de activos a proteger con su nivel de importancia identificados al igual que la lista de los factores de riesgo con su índice de probabilidad, se debe generar una descripción de las consecuencias que podría sufrir la empresa si los activos son afectados por sus respectivos factores de riesgo, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en qué grado son efectivas estas medidas.

Tabla 2.1: (Consecuencias y Medidas)

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)

2.2.1.2.5.- Cálculo de niveles de vulnerabilidad y porcentaje de riesgos

Una vez obtenidos los datos anteriores es posible estimar la probabilidad de ocurrencia que cada uno de los factores de riesgo representaba con respecto a los activos listados, considerando para esta estimación las medidas tomadas por la Institución para mitigar su acción.

Cuando se calculan los niveles de vulnerabilidad o niveles de riesgo en los que incurre cada activo se debe tener en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos.

Para valorar los activos, teóricamente, cualquier escala de valores es factible. A efectos prácticos es sin embargo muy importante que se use una escala común para todas las dimensiones, permitiendo comparar riesgos. Con ello se ha elegido una escala detallada

de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable a efectos de riesgo.

Tabla 2.2: (Criterios de Valoración)[8]

Valor		Criterio
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Para realizar el cálculo de lo niveles de vulnerabilidad se desarrollaron las siguientes operaciones:

- **Probabilidad De Ocurrencia**: Representan la probabilidad de que ocurran los factores de riesgo mencionados, en una escala del 1 al 3. Esta probabilidad debe ser evaluada teniendo en cuenta las medidas de seguridad existentes en la Institución.

- **Porcentaje De La Probabilidad Del Riesgo**: Se calcula el porcentaje de probabilidad de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo intervinientes para dicho activo. Esto es debido a que cada activo está afectado por un número diferente de riesgos posibles, de manera que este cálculo sirve para obtener un porcentaje de probabilidades equilibrado por

[8] MAGERIT Ver 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Catalogo-v10

igual para cualquier activo, independientemente de la cantidad de factores de riesgo que lo afectan.

- **Nivel De Vulnerabilidad**: Es aquí donde interviene el nivel de importancia, multiplicando al porcentaje de probabilidad del riesgo. De esta forma se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo. La suma de estos valores es el nivel de vulnerabilidad total que corresponde a cada activo.

$$Nivel\_de\_vulnerabilidad = (\%probabilidad\_de\_riesgos \times nivel\_de\_importancia)$$ [9]

$$\%probabilidad\_de\_riesgos = \frac{probabilidad\_de\_ocurrencia \times 100}{cantidad\_de\_factores\_de\_riesgos}$$

Tabla 2.3: (Cálculo de niveles de probabilidad)

N"Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	%Prob.riesgos	Nivel de vulnerabilidad
Cantidades de factores de riesgos =						

[9] www.segu-info.com.ar - Seguridad Informática/Evaluación de Riesgos

Tabla 2.4: (Niveles de Vulnerabilidad)

Activos	Niveles de Vulnerabilidad					
	Imp (1 - 10)	R %	Imp (1 - 3)	R %	Imp (1-1)	R %

2.2.1.2.6.- Análisis de importancias

En el análisis de importancias se tiene en cuenta el nivel de vulnerabilidad obtenido con una ponderación de la importancia de 1 a 10, se calculará el porcentaje de los riesgos y el porcentaje de la importancia. Al calcular la diferencia entre estos porcentajes (Dif. de %) se obtiene el porcentaje que muestra cuán sobrevaluados o menospreciados están los activos de acuerdo a sus riesgos.

El cálculo de los porcentajes antes mencionados se los detalla a continuación:

- Para aplicar la diferencia de porcentajes a la importancia actual, se multiplican.

Imp. x Dif. de %

- Este resultado no está en escala de 1 a 10, por lo que con una regla de tres simple, se centran los valores:

100 % ---------- - 10 puntos de importancia

Imp. x Dif. de % ---------- ? (= Diferencia de importancia)

- A este resultado se le suma (o resta de acuerdo al signo) a la importancia actual, obteniendo la importancia que debería tener cada activo (importancia ideal), de acuerdo al nivel de riesgos encontrado.

Importancia ideal = Importancia actual + Diferencia de importancia

Tabla 2.5: (Análisis de Importancias)

Activos	Nivel de vulnerabilidad	%	Importancia (actual)	%	Dif. de %	Dif. De Imp.

2.2.1.2.7.- Valores máximos y mínimos reales

El determinar los valores máximos y mínimos de vulnerabilidad que pueden obtener los activos cuando las probabilidades son llevadas a puntos extremos permite hacer una comparación con los valores de los Riesgos totales por cada activo. Estos cálculos se realizan sin tener en cuenta la influencia de la importancia, es decir se representan exclusivamente las debilidades de cada activo, con las medidas de seguridad que actualmente existen en la empresa.

Tabla 2.6: (Valores máximos y mínimos reales)

Activos - Riesgos totales (Sin ponderar la importancia)	Valores Máximos		Valores Mínimos		Valores Actuales	
	(333)	%	(111)	%	(123)	%

2.2.1.2.8.- Porcentajes de riesgos cubiertos

Como consecuencia de la comparación de los valores máximos y mínimos con los riesgos totales por activo, se puede calcular el porcentaje de riesgos descubiertos, el porcentaje de riesgo mínimo y la desviación que hay entre éstos, es decir, el nivel mínimo de riesgos posible.

Tabla 2.7: (Porcentajes de riesgos cubiertos)

Riesgos descubiertos:	
Riesgos mínimos:	
Riesgos a minimizar:	

2.2.2.- Lineamientos de Seguridad

2.2.2.1.- Definición

Los lineamientos de seguridad informática constan de documentos múltiples que se aplican a todas las áreas de la Institución que utilizan la información. Estos estándares abarcan controles de seguridad físicos, administrativos y lógicos (técnicos) que están diseñados para proteger la información. Los documentos de estándares definen el contenido y presentación de toda la documentación de seguridad de la Institución de manera que muchas instituciones contaran con docenas de documentos de los estándares para la seguridad de información.

2.2.2.2.- Norma ISO 17799

La norma ISO 17799:2000 presenta normas, criterios y recomendaciones básicas para gestionar la seguridad de la información de una organización, de tal forma que le permita en todo momento garantizar la confidencialidad, integridad y disponibilidad de la información que maneja.

2.2.2.3.- Selección de controles

Una vez realizado el Análisis de Riesgos previa la obtención de la situación actual de la Institución, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable. Los controles pueden seleccionarse sobre la base de estándares, o pueden diseñarse nuevos controles para satisfacer necesidades específicas conforme sea apropiado[10].

2.2.3.- Políticas

2.2.3.1.- Definición

Las políticas son instrucciones o principios determinados por los responsables directos o indirectos de un sistema que trazan una dirección que describen la manera de manejar un problema o situación, las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías.

Así como, las políticas no sólo son distintas, sino que se encuentran a un nivel mucho más alto que los procedimientos. La declaración de una política describe los lineamientos generales que deben seguirse para atender un problema específico, mientras que los procedimientos dictan los pasos operativos específicos o los métodos manuales que los trabajadores deben emplear para lograr un objetivo dado.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Es importante que las políticas de seguridad deben redactarse en un lenguaje

[10] Norma ISO/IEC 17799

sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: cambios en la infraestructura computacional, desarrollo de nuevos servicios, etc. Existen algunas políticas de seguridad[11]:

- Políticas administrativas.- Se establecen aquellos procedimientos de carácter administrativo en la organización, así como, las responsabilidades compartidas por todos los usuarios.
- Políticas de control de acceso
    - Política de menor privilegio.- Acceso estricto a objetos determinados, con mínimos privilegios para los usuarios.
    - Política de compartición.- Acceso de máximo privilegio en el que cada usuario puede acceder a todos los objetos.
    - Granularidad.- Número de objetos accesibles.
- Políticas de control de flujo.- se refiere a la información a la que se accede, se envía y recibe.

2.2.3.2.- Por qué tener políticas escritas

Existen varias razones por las cuales es recomendable tener políticas escritas en una organización[12]:

- Para cumplir con regulaciones legales o técnicas.

[11] Libro Electrónico de Seguridad Informática y Criptografía Versión v 4.0

[12] http://www.unal.edu.co/seguridad/documentos/guia_para_elaborar_politicas_v1_0.pdf

- Como guía para el comportamiento profesional y personal.
- Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares.
- Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo.
- Permite encontrar las mejores prácticas en el trabajo.
- Permiten asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto).

2.2.3.3.- Fases

2.2.3.3.1.- Fase de Desarrollo

Durante esta fase la política será creada, revisada y aprobada.

2.2.3.3.1.1.- Etapa de Creación

El primer paso en la fase de desarrollo de una política es la etapa de creación en la cual se debe planificar, investigar y redactar la política y por último crear la política como tal. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la Institución.

2.2.3.3.1.2.- Etapa de Revisión

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez que la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo independiente para su evaluación antes de su aprobación final. Propio de esta etapa es la presentación de la política a los revisores, exponiendo cualquier punto que puede ser importante para la revisión, como parte de esta función se espera recopilar comentarios y las recomendaciones para realizar

cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener su versión final.

2.2.3.3.1.3.- Etapa de Aprobación

El paso final en la fase de desarrollo de la política es la aprobación, que permite iniciar la implementación de la política.

2.2.3.3.2.- Fase de Implementación

En la fase de implementación la política es comunicada y acatada (o no cumplida por alguna excepción)

2.2.3.3.3.- Fase de Mantenimiento

En esta fase los usuarios deben ser concientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

2.2.3.3.4.- Fase de Eliminación

En la fase de eliminación, si una política no es requerida se la retira.

2.3.- Arquitectura de Seguridad

2.3.1.- Definición

Una Arquitectura de Seguridad de la Información global y flexible implantada en toda la organización es el primer paso necesario realizar para proteger la confidencialidad, integridad y disponibilidad de la información y los recursos del sistema. Los programas de seguridad más eficaces son aquellos que cuentan con una participación activa desde dentro de la organización. Fuentes externas pueden proporcionar conocimientos y experiencia

específica. No obstante, el programa de seguridad en sí debe ser dirigido y gestionado internamente.

La Arquitectura de Seguridad es necesaria en los entornos actuales de proceso distribuido, en los que todo el mundo tanto dentro de la organización como externo a la misma tiene una responsabilidad en la seguridad de los sistemas y redes a las que tiene acceso. Los controles implantados deben incluir una combinación de procedimientos administrativos, físicos y técnicos que se seleccionan en función de los tipos de amenazas y el riesgo real estimado.

La organización debe empezar por reconocer la importancia de la seguridad al nivel de dirección en que se pueden asignar recursos adecuados para implantar los procedimientos con eficacia.

2.3.2.- Áreas de Seguridad

2.3.2.1.- Seguridad Lógica

La Seguridad Lógica consiste en evaluar los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.3.2.2.- Seguridad Física

La Seguridad Física consiste en evaluar que el centro de cómputo, los equipos, los dispositivos, los medios de almacenamientos y las personas que conforman el sistema informático de la organización cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

2.3.2.3.- Seguridad de Aplicaciones

La Seguridad de Aplicaciones evalúa las aplicaciones utilizadas en la organización, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

2.3.2.4.- Seguridad de Comunicaciones

La Seguridad de Comunicaciones deberá evaluar, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

Capítulo 3. Diagnóstico de la Situación Actual

3.1.- Guía Metodológica

Para obtener la situación actual de la Armada del Ecuador en cuánto a la Seguridad Informática se planteó el siguiente esquema:

- Conocimiento general de la Armada del Ecuador (Misión, Visión, Estructura Organizacional)
- Conocimiento de la misión, visión y estructura orgánica de la Dirección de Desarrollo Administrativo e Informático
- Técnicas y Herramientas
  - Revisión analítica de documentos (Plan Estratégico, Manual Organizacional, Manual de Políticas y Normas, etc)
  - Cuestionarios
  - Análisis de Riesgos
- Conclusiones del Diagnóstico

3.1.1.- Descripción General de la Armada del Ecuador

3.1.1.1- Visión de la Armada del Ecuador

Una Armada con poder Naval disuasivo, altamente entrenada y lista para la victoria. Involucrada totalmente con el desarrollo y proyección de los intereses marítimos; constituida por hombres de elevada calidad profesional y moral, que basa su institucionalidad en el cumplimiento de valores y principios fundamentales.

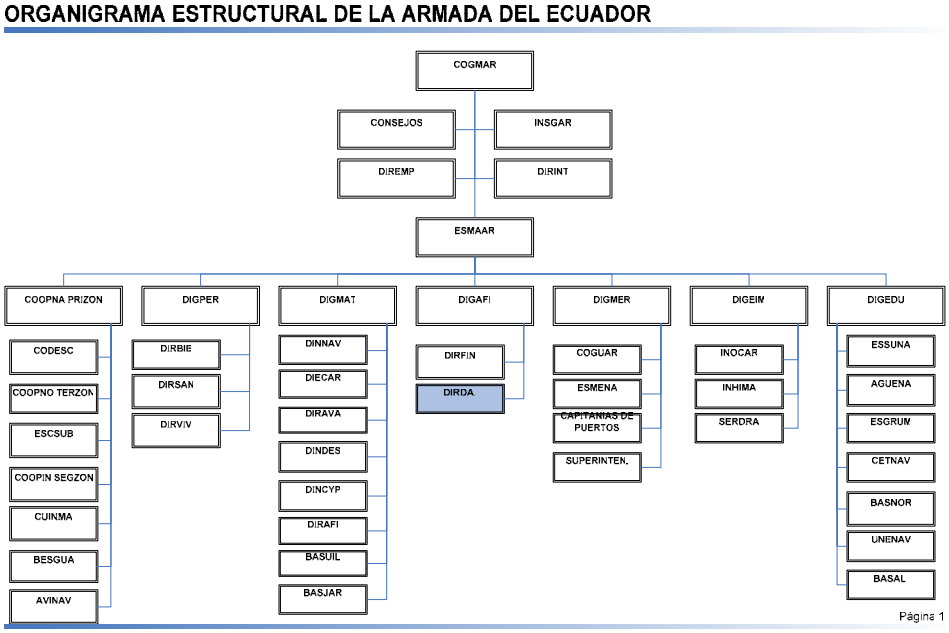
3.1.1.2- Misión de la Armada del Ecuador

Organizar, entrenar, equipar y mantener el poder Naval; así como participar en los procesos que garanticen la seguridad de la Nación y propendan a su desarrollo, con la

finalidad de contribuir a la consecución y mantenimiento de los objetivos nacionales de acuerdo a la planificación prevista para tiempos de paz, de conflicto y de guerra.

3.1.1.3.- Organigrama Estructural de la Armada del Ecuador

Cuadro 3.1: (Organigrama Estructural de la Armada del Ecuador)

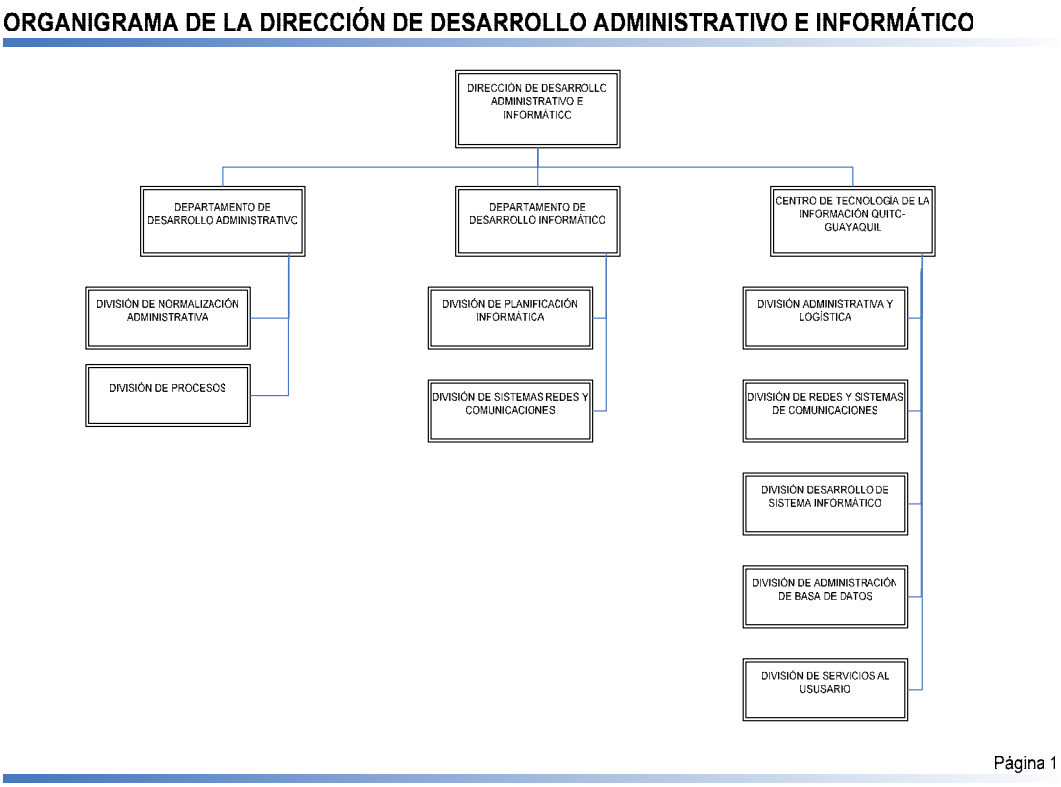


3.1.1.4.- Descripción General de la Dirección de Desarrollo, Administrativo e Informático (DIRDAI)

Planificar, desarrollar, normalizar, mantener la base administrativa de la Institución, así como la sistematización y automatización de los sistemas y procedimientos administrativos que permitan racionalizar y facilitar el reordenamiento de la gestión institucional a través de la implementación de la tecnología informática y de comunicaciones, considerando las políticas del mando y el Plan Estratégico Institucional.

3.1.1.4.1.- Organigrama Estructural de la DIRDAI

Cuadro 3.2: (Organigrama Estructural de la DIRDAI)



3.1.2.- Especificación de Técnicas y Herramientas

La finalidad de utilizar técnicas y herramientas dentro de la elaboración de un Manual de Seguridades Informáticas es la de obtener evidencia física para la elaboración del Diagnóstico de la Situación Actual de la Institución y así analizar los posibles riesgos y amenazas a la que está expuesta, con ello poder determinar políticas y estándares dentro de su Arquitectura de Seguridades Informáticas que para el caso de estudio se aplicará a la Armada del Ecuador. Para ello se utilizaron las siguientes técnicas y herramientas:

Técnicas:

- Estudio general de la Armada del Ecuador y de la Dirección de Desarrollo Administrativo e Informático
- Análisis de la documentación como:
    - Plan Estratégico de Tecnologías de Información
    - Manual Organizacional de la Armada del Ecuador
    - Manual Organizacional de la DIRDAI
    - Situación Tecnológica Informática de la Fuerza Naval
    - Planes de Contingencias
    - Diagramas topológicos de Red e Instalaciones Físicas
- Confirmación de los hechos recopilados en cuestionarios o entrevistas
- Observación de las instalaciones, sistemas, cumplimiento de normas y políticas
- Entrevistas al personal de la DIRDAI
- Conocimiento técnico y Administrativo sobre el Marco Teórico para la elaboración de un Manual de Seguridades Informáticas.

Herramientas:

- La aplicación de los cuestionarios se oriento a la DIRDAI por ser la encargada del soporte técnico, desarrollo administrativo informático, y de comunicación de datos de la Armada del Ecuador y específicamente a los dos Centros Tecnológicos Informáticos de Quito y Guayaquil (CETEIQ, CETEIG).
- Un detalle a destacar es la identificación del nombre del encuestado en los diferentes cuestionarios realizados, con el fin de avalizar la información proporcionada. Ver Anexo A

- Otra herramienta utilizada es el Análisis de Riesgos la misma que permitirá identificar los riesgos como sus consecuencias en los diferentes activos informáticos organizacionales.

3.1.3.- Diagnóstico

La no aplicación de la estadística dentro del análisis de los cuestionarios se debe a que no se va realizar una recopilación de datos por el número de ocurrencias de un determinado factor o recopilar datos de una población[13] basados en una muestra[14], sino, determinar la Situación Actual de la Institución identificando los riesgos a los que se encuentran expuestos sus activos. Cabe destacar que en el levantamiento de información realizado a partir de los cuestionarios se hizo un análisis por pregunta clasificándolas de acuerdo a las variables de Seguridad Informática, Confidencialidad, Integridad, Disponibilidad, Autenticación y No-Repudio, especificadas en el Capítulo 1 y con ello poder establecer políticas que nos ayuden a minimizar los riesgos encontrados.

3.1.3.1.- Confidencialidad

En ambos Centros Tecnológicos el encargado de realizar los cambios de contraseñas es el Administrador de Redes y de Comunicaciones.

En lo referente a la creación de contraseñas, los usuarios de las dependencias administradas por el CETEIG son entrenados a no divulgarlas, en cambio el CETEIQ entrena a sus usuarios a no guardarlas en lugares donde se puedan encontrar, a no usar contraseñas fáciles de descifrar y a no divulgarlas.

[13] Población: Conjunto de todos los posibles individuos, objetos o medidas de interés. (Estadística para Administración y Economía- Mason)

[14] Muestra: Una porción, o parte, de una población de interés. (Estadística para Administración y Economía- Mason)

Se restringe el acceso en el Centro de Cómputo a la gente que no pertenece al departamento. Mediante tarjetas de entradas en ambos Centros Tecnológicos, y solo circuito cerrado de cámaras en el CETEIQ.

Todo usuario de las dependencias administradas por los Centro de Tecnología tiene la posibilidad de instalar, enchufar una impresora o cualquier dispositivo en una máquina.

El almacén de cintas de backup de ambos Centros Tecnológicos son asegurados mediante llaves.

En el Centro de Tecnológico de Quito existe fuera de la red interna información valiosa, a diferencia de Guayaquil.

La confidencialidad de los datos en una laptop depende del responsable o encargado de la máquina.

El control de acceso de las bases de datos es controlado solo por el responsable de esa área en ambos Centros Tecnológicos, y solo en Quito controlan el número de intentos fallidos de conexión a las bases de datos, como la modificación de los datos.

En las máquinas de la Institución solo los administradores de los Centros Tecnológicos pueden modificar las carpetas del Sistema.

En el caso de que existiera la participación de terceros en el desarrollo de un sistema el código fuente si queda en el CETEIG, en el CETEIQ el código fuente no se queda en la Institución después del desarrollo de un sistema.

Dentro del control de envío de archivos confidenciales, u otros archivos que ameritan seguridad se basan en las políticas establecidas en el documento oficial RT3 IV.99 en donde se toma muy en cuenta que todo archivo o mensaje se debe proteger en aspectos de Integridad, Confidencialidad, Autenticación.

3.1.3.2.- Integridad

En el CETEIQ se realiza la actualización, revisión y asignación a los usuarios en un grupo determinado con sus respectivos permisos. En el CETEIG esto no se realiza.
Los usuarios predeterminados por los sistemas operativos son eliminados por el CETEIQ, a diferencia del CETEIG.

Las contraseñas con creadas por los usuarios en la Armada del Ecuador con un mínimo de seis caracteres siendo solo alfa-numéricos en las dependencias administradas por el CETEIG, y de numéricos, alfa-numéricos y caracteres especiales en las dependencias administradas CETEIQ.

En ambos Centros de Tecnología cuando existe más de una cuenta de Administrador las contraseñas no son las mismas.

Las contraseñas de usuarios son cambiadas cada mes por motivos de seguridad, si el caso amerita estas pueden ser cambiadas en cualquier momento.

El CETEIQ para mantener la integridad y la confiabilidad de los datos en las diferentes dependencias que administre sigue procedimientos como: el control de acceso para limitar lo que se lee, borra, modifica, prohíben el acceso público a las bases de datos, verifican que los programas y la información pública no tenga virus, y mantienen separados los datos que se publican en el Internet de los datos del interior de la empresa. El CETEIG solo verifica que los programas y la información pública no tengan virus.

Todas las máquinas tienen habilitados los dispositivos externos, como la lectora de Cd's y disquetera, así como se controlan los virus de estos dispositivos mediante el antivirus.

En la elaboración de la estructura de los edificios no se tuvo en cuenta la seguridad de los datos y equipos en ambos Centros Tecnológicos.

El CETEIQ se encuentra ubicado en el subsuelo, en cambio el CETEIG está ubicado en pisos elevados para evitar inundaciones.

Como política de seguridad para los Centros de Cómputos esta prohibido comer, fumar y beber dentro de él.

En el CETEIG los canales de red fueron ubicados en un lugar seguro de inundaciones, cortes eléctricos, en el CETEIQ no se prevee la seguridad de los canales de red en el caso de una inundación ya que el Centro se encuentra ubicado en el subsuelo del edificio principal de la Institución.

No se tienen en cuenta los distintos riesgos que se someten los datos de la Institución cuando se utiliza laptos o PC`s.

El CETEIQ dispone de un Plan de Contingencias basado en las dependencias que administra, en el CETEIG no se ha desarrollado un Plan de Contingencias basado en las dependencias que administra, pero ambos realizaron un previo análisis de riesgos antes de la realización del plan.

El Plan de Contingencias que controla el CETEIQ incluye un Plan para recuperación de desastres, reducción de riesgos y la definición de responsabilidades y funciones de las personas que están incluidas en el Plan, pero no se realiza constantemente su actualización cuando surge algún cambio en puestos, funciones o amenazas. Así como no poseen acciones defensivas en caso de violación interna o externa.

No existe entrenamiento para los responsables del Plan de Contingencias tampoco para los usuarios en el CETEIQ.

El CETEIQ dispone de un Plan de recuperación de desastres con responsabilidad asignada para cada miembro del equipo, en el CETEIG no tienen un Plan de recuperación de desastres.

En el CETEIQ existen procedimiento para realizar el backup de datos en caso de emergencia el responsable es el Administrador de la Red, este procedimiento se encuentra incluido en el Plan de Contingencias. El personal no ha sido entrenado para enfrentar un siniestro.

En ambos Centros Tecnológicos después de que haya sucedido un desastre se evalúan la magnitud del daño y cuales fueron los sistemas afectados.

El CETEIQ controla los cambios de los archivos del sistema o base de datos de las dependencias que administra, así como las restricciones de datos de salida como portapapeles o impresoras.

En los equipos de la Institución se almacenan los archivos del sistema y los de trabajo en directorios separados para evitar cualquier pérdida importante de información en caso de algún daño en el sistema.

En la Institución se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones. Las variables, parámetros de cálculo se incluyen en archivos separados de los programas para facilitar su modificación, existiendo un control de cambios en el desarrollo.

El CETEIQ dispone de procedimientos para detectar programas que no deberían estar en los equipos de trabajo, ya sea por problemas de licencias o virus que posiblemente son bajados desde la Web.

En ambos Centros Tecnológicos se desarrollan aplicaciones para cada área de la Institución, usando una metodología estándar para su desarrollo, así como la implementación de mecanismos de seguridad durante sus fases.

Se usan métricas durante el desarrollo del sistema en el CETEIQ, en el CETEIG no se usan métricas.

Cualquier usuario está permitido para crear carpetas compartidas.

No se realiza pruebas de los puertos para verificar si permanecen habilitados o no de acuerdo a las normas establecidas. Ni tampoco se realiza un chequeo periódico de la red y sus permisos en el CETEIG.

Para el control de virus ambos Centros Tecnológicos poseen procedimientos como paquetes de software, firewalls, monitoreo para evaluar anomalías en la red, creación de discos de rescate y respaldo de datos.

El CETEIG no dispone de mecanismos que filtren el correo electrónico que ingresa a la institución.

El CETEIQ realiza un análisis de virus en sus servidores de manera semanal a diferencia del CETEIG que no lo realiza.

3.1.3.3.- Disponibilidad

En el CETEIQ el Active Directory es utilizado como herramienta para el control de acceso lógico y para las restricciones de servicio en base a usuarios, aplicaciones y departamentos.

La restricción de interfaz que ven los usuarios esta controlada mediante el Active Directory por el CETEIQ en sus diferentes dependencias. El CETEIG no maneja este tipo de control de acceso interno.

Los servidores que se encuentran en los Centros de Tecnología de Información se mantienen prendidos las 24 horas del día, y solo en el CETEIG se los reinician quincenalmente.

En el Centro de Cómputo de Quito se mantiene y revisan los aparatos como aire acondicionado, los detectores de humo y la luz de emergencia, y en el caso de Guayaquil solo se mantienen y revisa el aire acondicionado.

Se dispone de un UPS para el funcionamiento diario de las máquinas y se han realizado pruebas de máxima carga para su comprobar su capacidad de rendimiento.

Se disponen extintores de incendio en lugares visibles pero el personal no conoce la forma de su utilización.

En ambos Centros Tecnológicos no disponen de rociadores en caso de emergencia de algún incendio, así como las máquinas no poseen ninguna protección para la lluvia artificial.

En el CETEIQ se dispone de un dispositivo para evitar la sobrecarga de la red eléctrica, y se revisan posibles fallas eléctricas o posibles causas de incendio, en el CETEIG no disponen de un dispositivo para evitar la sobrecarga de la red eléctrica.

En el CETEIG el cableado para los equipos esta ubicado en el techo falso, en cambio en el CETEIQ se lo realizo debajo del piso falso. Para la estructuración del cableado se baso en el modelo de una norma.

La estructuración de la red fue diseñada para anticipar su crecimiento y reinstalaciones de equipos en ambos Centros de Tecnología. Así como la ubicación del Backbone central de la red tanto de Guayaquil y Quito se encuentra ubicado en los respectivos Centros Tecnológicos.

En caso de unas emergencias en ambos Centros Tecnológicos no disponen de un interruptor de energía de emergencia para la puerta de salida.

Ambos Centros Tecnológicos tienen procedimientos para rotulación, manipulación y dar de baja a las computadoras de las distintas dependencias, así como sus periféricos y medios de almacenamiento removibles y no removibles.

En el CETEIQ se realizan los backup de los datos diariamente o semanal cada vez que lo necesite, a diferencia del CETEIG que no realiza backup.

Para la realización del backup de hardware ambos Centros Tecnológicos contratan terceros que proporcione los insumos necesarios en caso de emergencia.

En el CETEIQ disponen de una herramienta de backup automáticas y almacenan estos datos dentro del edificio y en el CETEIG que no disponen de una herramienta automática y si se almacenan los backup en lugares externos al edificios.

En ambos Centros Tecnológicos disponen del backup de las páginas Web y sus actualizaciones.

En ambos Centros Tecnológicos no manejan un tipo de mecanismo de reportes para el manejo de incidentes.

No existe ningún Centro Tecnológico Alternativo que cumpla las mismas funciones de los principales de Quito y Guayaquil.

En el CETEIQ se ha realizado una lista de datos, elementos de hardware y software críticos a proteger en la Institución, situación que no se ha realizado en Guayaquil.

En ambos Centros Tecnológicos no existe un equipo de evaluación para corregir y documentar los errores, que sirva para generar un Plan de Contingencias.

En el CETEIG tienen identificados todos los sistemas de información con sus características, y en el CETEIQ se almacenan algunos datos como nombre, lenguaje, departamento que usa y generan la información, como el equipamiento mínimo.

En el CETEIQ se ha realizado el inventario de equipos de cómputo como de hardware, software, archivos principales, y la configuración de los equipos. Solo de hardware y software en el CETEIG. Ambos Centros no disponen de pólizas de seguro para los equipos de la Institución en caso de un siniestro.

En el Plan de emergencia que disponen en el CETEIQ se incluyen los siguientes puntos como: vías de salida, plan de evacuación del personal, plan de puesta a buen recaudo de los activos, ubicación y señalación de los elementos contra el siniestro, pero no se han tomado en cuenta los distintos escenarios posibles.

Los Centros Tecnológicos tienen la responsabilidad de dar publicidad a las nuevas Normas de Seguridad del área de sistemas, pero la mayoría de los empleados no tienen conocimiento de la existencia de un Plan de Contingencias.

Disponen de documentación detallada sobre el equipamiento informático como distribución física de las instalaciones e inventario de hardware y software.

No existe una concientización de la seguridad informática por parte del personal de la Institución.

En los distintos equipos de cómputo de la Armada del Ecuador se encuentra instalados los Sistemas de Operativos de Windows como de Linux, en sus distintas versiones.

Ambos Centros Tecnológicos ajustan el sistema operativo a estándares internacionales en los equipos existentes en la Institución, así como disponen de manuales propios del software.

Todos los equipos de la Institución manejan la misma versión de programas. Así como la configuración de los equipos es estandarizada, por lo tanto existen controles para

la instalación y actualización de los parches de las aplicaciones, para su correcto funcionamiento.

Ambos Centros etiquen y almacenan los instaladores de los programas y drivers, en lugares seguros con su responsable.

En el CETEIG se forma una mesa de reportes donde se identifican usuarios con incidentes de seguridad.

En el CETEIQ se borran los archivos, programas o servicios innecesarios para que no llenen los discos de los equipos con basura, y así no provocar la caída del sistema, en el CETEIG se dejan almacenados los programas, archivos o servicios innecesarios en los equipos.

En la etapa de implementación del sistema se toman medidas de seguridad para su ejecución. En el CETEIQ se documentas las pruebas y los resultados de los sistemas y en ambos Centros Tecnológicos se realizan el mantenimiento en los sistemas.

De los sistemas desarrollados se almacena: la fecha de implementación, analista y programador responsable, objetivos, diagramas de flujo, archivos de entrada- salida que se utiliza y el manual de usuario.

La topología de red predominante es la topología Estrella variando su tipo entre 568A, 568B, Fast Ethernet, Giga Ethernet dependiendo de la conexión de los diferentes repartos administrados por sus correspondientes Centros de Tecnología. También hay presencia de topología en Bus en pocos repartos.

La conexión entre los dos Centros Tecnológicos es mediante un E1 de 2048 KPBS, dentro de la tecnología utilizada se encuentra Cable UTP, Fibra Óptica, Modem, inalámbrico.

No existen medios alternativos de transmisión de datos en caso de que exista alguna contingencia con la red en ambos Centros Tecnológicos.

En el CETEIG disponen servidor de Proxy, Mail y Firewall más no un servidor de Dominio, Base de Datos y Aplicaciones. Disponen también de un servidor de Proxy como respaldo.

En el tema de correos electrónicos el CETEIG no dispone de direcciones para todo el personal y no se controla el correo basura.

El CETEIG permite la utilización del servicio de Chat como el Messenger y el Yahoo así como la descarga de archivos mediante estos servicios. El CETEIQ utiliza el servicio de Chat Jabber solo para uso interno.

3.1.3.4.- Autenticación

Los datos almacenados en los perfiles de usuarios para el control de seguridad en el CETEIQ son: ID de usuario, nombre y apellido completos, puesto de trabajo y departamento de la Institución, tipo de cuenta o grupo al que pertenece, fecha de expiración de la cuenta, datos de los permisos de acceso y excepciones. A diferencia del CETEIG solo controla el ID de usuario y el tipo de cuenta o el grupo al que pertenece.
El ID de usuario no se puede repetirse en los diferentes repartos.

Cuando el usuario se encuentra en un período de inactividad ya sea en el sistema o en el Pc, el CETEIQ solicita al usuario que ingrese su contraseña para su activación. En el CETEIG no maneja este tipo de seguridad.

El encargado de la asignación de permisos a los usuarios es el Administrador de Red y la clasificación de los recursos (datos) esta basado por departamentos.

La conformación de grupos de usuarios en CETEIQ se lo realiza por el rol que desempeñen, en el CETEIG por el departamento al que pertenezca.

En el CETEIG existe un Administrador de Redes y Comunicaciones y cuatro Administradores de Aplicaciones. En el CETEIQ existe un Administrador Base de Datos, y dos Administradores que manejan el Área de Redes, Comunicaciones y Aplicaciones.

La autenticación de usuarios por el CETEIQ a la red interna se lo realiza mediante el nombre de usuario, la contraseña y el grupo o entorno de red al que pertenece, en el CETEIG se lo realiza por nombre de usuario, contraseña y estación de trabajo.

Se utiliza el ID de usuario para el control de acceso a los recursos, asignados por el CETEIQ y para el ingreso al sistema. Y solo para el ingreso a los recursos en el CETEIG.

Los datos de autenticación de la Armada del Ecuador administrados por los Centros Tecnológicos, como las contraseñas, se lo realiza de manera confidencial, encriptados y en el caso del ingreso de la contraseña a la red se presenta en pantalla con asteriscos.

Quien tiene acceso a los datos de autenticación en el CETEIQ son el Administrador de Redes y Comunicaciones, y el Administrador de Base de Datos. En el CETEIG lo realiza el Administrador de Redes y Comunicaciones y el Administrador de Aplicaciones.

La autenticación de usuarios en las dependencias administradas por el CETEIQ se lo realiza para una aplicación en particular y para la red LAN, en el CETEIG solo para una aplicación en particular en sus dependencias administradas.

Cuando un usuario de las diferentes dependencias administradas por el CETEIQ se autentifica de manera errónea la cuenta de usuario es bloqueada después de tres intentos.

No se usan firmas digitales para autenticar los usuarios dentro de la Armada del Ecuador cuando mandan mensajes internos o externos.

Cuando un usuario de las dependencias administradas por el CETEIQ ingresa con su cuenta por primera vez al sistema o a la red ésta aparece como expirada para que el usuario ingrese su nueva contraseña. En el CETEIG no se maneja este tipo de seguridad.

Para el control de acceso externo ambos Centros Tecnológicos utilizan Gateways o Firewalls que permiten el acceso o no a los datos.

Como procedimiento al posible ingreso de un intruso el CETEIQ documenta, da seguimiento correctivo y verifica que implicaciones pudo tener en la empresa, a diferencia del CETEIG, no realiza ningún tipo de procedimiento. Es de destacar que ninguno de los dos Centros Tecnológicos utiliza herramientas para detectar intrusos en la red.

En el CETEIG no controlan las entradas no autorizadas en las estaciones de trabajo o puertos lógicos, el CETEIQ si controla las entradas no autorizadas a las estaciones de trabajo o puertos lógicos.

Las claves de autentificación del servicio de correo electrónico son de conocimiento de los usuarios en ambos Centros Tecnológicos.

3.1.3.5.- No-Repudio

Los históricos de las actividades de los usuarios en el sistema son controlados por el CETEIQ, el CETEIG no maneja un control de los históricos de las actividades realizadas por los usuarios.

Cuando los usuarios de las dependencias administradas por el CETEIQ logra autenticarse, se almacena la fecha, hora y localización de la última conexión realizada, y solo la localización en la última conexión realizada en las dependencias administradas por el CETEIG.

En el Centro de Cómputo se realizan chequeos en el sistema, extraen logísticos sobre las conexiones de red levantadas, intentos de ingresos desde el exterior de la red interna, conexiones externas realizadas desde la red.

En ambos Centros Tecnológicos se realizan históricos de las modificaciones en los sistemas durante su desarrollo y mantenimiento, se almacenan datos como: nombre del sistema afectado, fecha de modificación, persona que realizó el cambio y descripción de la

modificación en el caso de CETEIQ, en el CETEIG solo se almacena fecha y persona que realizó la modificación.

3.1.4.- Análisis de riesgos

El presente análisis de riesgo fue desarrollado con el propósito de determinar cuáles de los activos de la Institución tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, y considerando el grado en que el riesgo puede ser controlado.

3.1.4.1.- Listado de activos y asignación de prioridades

Una vez realizado el levantamiento de información y posteriormente la situación actual de la Institución, se identificaron sus activos considerados vitales por el nivel impacto que representan a la misma en el caso de si fallara o faltase. Por tal motivo se generó un listado de los mismos, en el cual se asignó y clasificó a cada uno de los activos, por su nivel de importancia (Escala 1- 10) siendo el valor de 10 como el activo de mayor importancia.

Tabla 3.1: (Listado de activos con su nivel de importancia)

Activos a proteger	**Importancia**
Servidores	10
Bases de datos	10
Software de aplicación, programas fuente, sistemas operativos	9
Backup (respaldos de hardware, software y datos)	9
Datos en transito, datos de configuración, datos en medios externos	8
Administradores (Centros Tecnológicos)	7

Cableado, antenas, switches, hubs, modems, routers, firewalls	6
Red	6
Usuarios	5
Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4
Hardware (teclado, monitor, unidades de discos, medios removibles,etc.)	3
Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	2
Datos de usuarios	1

3.1.4.2.- Identificación de factores de riesgos y asignación de probabilidades de ocurrencia.

A continuación se listaron los factores de riesgo relevantes a los pueden verse sometidos cada uno de los activos arriba nombrados con su probabilidad de ocurrencia en una escala del 1 al 3 o en su defecto Bajo – Medio - Alto.

Tabla 3.2: (Factores de riesgos con su probabilidad de ocurrencia)

Factores de riesgos	**Probabilidad de Ocurrencia**
Abuso de puertos para el mantenimiento remoto	1
Acceso no autorizado a datos (borrado, modificación, etc.)	2
Administración impropia del sistema de Tecnología de Información	1
Almacenamiento de contraseñas negligente	2
Ancho de banda insuficiente	1
Aplicaciones sin licencia	2
Ausencia o falta de segmentación	2
Borrado, modificación o revelación desautorizada o inadvertida de	1

información	
Complejidad en el diseño de las redes de sistemas de Tecnología de Información	1
Condiciones de trabajo adversas	1
Conexión de cables inadmisible	1
Configuración inadecuada de componentes de red	2
Configuración impropia del servicio de Mail	2
Conocimiento insuficiente de los documentos Institucionales	2
Conocimiento insuficiente de los requerimientos en el desarrollo de sistemas	3
Copia no autorizada a un medio de datos	2
Corte de luz, UPS descargado o variaciones de voltaje	1
Daño o destrucción de cables o equipos inadvertido	1
Deficiencias conceptuales en la red	1
Descripción de archivos inadecuada	1
Destrucción negligente de equipos o datos	1
Destrucción o mal funcionamiento de un componente	1
Desvinculación del personal	1
Documentación deficiente	3
Documentación insuficiente o faltante, Funciones no documentadas	3
Denegación de Servicio	1
Entrada sin autorización a departamentos o cubículos	2
Entrenamiento de usuarios inadecuado	2
Errores de configuración y operación (sistema)	1
Errores en las funciones de encriptación	1
Factores ambientales	1

Falla de base de datos	1
Falla del sistema	1
Falla en la LAN y WAN	1
Falla en medios externos	1
Falta de auditorias	3
Falta de autenticación	1
Falta de confidencialidad	1
Falta de cuidado en el manejo de la información (Ej. Password)	2
Falta de espacio de almacenamiento	1
Fraude	2
Incendios	3
Interferencias	1
Límite de vida útil - Máquinas obsoletas	1
Longitud de los cables de red excedida	1
Mal interpretación	2
Mal mantenimiento	1
Mal uso de derechos de administrador	3
Mal uso de servicios de mail	2
Mala administración de control de acceso	1
Mala configuración de las tareas programadas del backups	1
Mala evaluación de datos de auditoria	3
Mala integridad de los datos	1
Mantenimiento inadecuado o ausente	2
Medios de datos no están disponibles cuando son necesarios	1

Modificación e intercepción de datos en tránsito	1
Modificación no autorizada de datos	1
No-cumplimiento con las medidas de seguridad del sistema	2
Penetración, intercepción o manipulación de líneas de comunicación	1
Pérdida de backups	2
Pérdida de confidencialidad en datos privados y de sistema	1
Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	1
Pérdida de datos	1
Pérdida de datos en tránsito	1
Poca adaptación a cambios	1
Portapapeles, impresoras o directorios compartidos	1
Prueba de software deficiente	1
Recursos escasos	1
Reducción de velocidad de transmisión	1
Reglas insuficientes o ausencia de ellas	2
Riesgo por el personal de limpieza o personal externo	1
Robo	1
Robo de información	1
Robo por uso de laptops	1
Rótulos inadecuados en los medios de datos	1
Sabotaje	1
Seguridad de base de datos deficiente	1
Sincronización de tiempo inadecuada	1
Software desactualizado	1

Spoofing y sniffing	1
Transferencia de datos incorrectos o no deseados	1
Transporte inseguro de archivos	1
Transporte inseguro de medios de datos	1
Utilización de cuentas de usuario sin autorización	2
Uso de derechos sin autorización	2
Uso descontrolado de recursos (DoS)	1
Uso impropio del sistema de Tecnologías de la Información	1
Uso sin autorización	1
Visualización de información	1
Virus, gusanos y caballos de Troya	3

3.1.4.3.- Descripción de consecuencias

Teniendo presente el listado anterior, se generó una descripción de las consecuencias que podría sufrir la Institución si los activos son afectados por sus respectivos factores de riesgo, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en qué grado son efectivas estas medidas.

Para la elaboración de la tabla se utilizó las siguientes características:

- **Factores de Riesgo**: Indica los factores de riesgo a los que está expuesto el activo obtenidos de la lista de factores de riesgos antes especificados.
- **Consecuencias:** Impacto que se ve reflejado en el activo en ocurrencia del factor de riesgo expuesto.
- "**s**" si se protege el activo dentro de la Institución
- "**n**" si no se el activo dentro de la Institución.

- **Como:** Como protege la Institución el activo en análisis frente al riesgo expuesto.
- **Efectividad:** Parámetros establecidos de acuerdo a como la Institución maneja la protección del activo respecto a un riesgo. Se estableció una ponderación de: deficiente (**d**), mejorable (**m**), eficiente (**e**).

Aplicación de la Tabla 2.1: (Consecuencias y medidas)

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Servidores	Acceso no autorizado	Robo, modificación de información.	s	Seguridad física y control de acceso lógico	m
	Corte de luz, UPS descargado o variaciones de voltaje.	Falta de sistema.	s	Generador, UPS, estabilizador.	e
	Deficiencias conceptuales en la red	Mal funcionamiento de los servidores de mail, DNS	s	Capacitación y preparación a los Administradores	e
	Destrucción de un componente	Pérdida de tiempo por necesidad de reemplazo.	n		d
	Error de configuración	Aumento de vulnerabilidades e inestabilidad en el sistema.	s	Administrador de la Red y Comunicaciones	e
	Factores ambientales	Falta de sistema y destrucción de equipos.	s	Seguridad física	m
	Incendios	Pérdida de Información	s	Extintores, políticas de seguridad	m
	Límite de vida útil - Máquinas obsoletas	Deterioro en la performance del sistema.	s	Equipamiento actual y asesoramiento permanente.	e
	Mal mantenimiento	Interrupciones en el funcionamiento del sistema.	s	Mantenimiento interno	e
	Modificación no autorizada de datos	Inconsistencia de datos, mala configuración, fraude.	s	Controles de acceso físico y lógico al servidor.	m
	Robo	Pérdida de equipamiento o información.	s	Controles de acceso físicos, sistema de camaras, alarmas, guardia militar.	e
	Robo de información	Divulgación de información confidencial, y pérdida de datos	s	Tarjetas de seguridad para el ingreso al cuarto de servidores	m
	Virus	Fallas generales del sistema y en la red.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Bases de Datos	Copia no autorizada a un medio de datos	Divulgación de información.	s	Controles lógicos.	e
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de las Base de Datos	n		
	Falla de base de datos	Inconsistencias en los datos.	s	Controles internos y backup de los datos.	m
	Falla en medios externos	Perdida de backup.	s	Redundancia de los mismos.	m
	Falta de espacio de almacenamiento	Falla en la aplicación.	s	Recursos abundantes.	e
	Fraude	Modificación de información sin autorización	s	Políticas y normas internas	m
	Incendios	Pérdida de Base de Datos	s	Uso de extintores	m
	Mala configuración de las tareas programadas de backups	Datos sin backup.	s	Organización de las tareas programadas.	e
	Mala integridad de los datos	Inconsistencias y redundancia de datos.	s	Controles en las aplicaciones desarrolladas.	m
	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo y productividad.	s	Controles lógicos del funcionamiento de la base	m
	Pérdida de backups	Incapacidad de restauración	n		d
	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información.	s	Controles físicos y controles de accesos lógicos a datos críticos.	m
	Perdida de datos en tránsito	Inconsistencia de datos y divulgación de información.	s	Políticas de configuración de red.	m
	Portapapeles, impresoras o directorios compartidos	Divulgación de información.	s	Controles lógicos.	d
	Reglas insuficientes o ausencia de ellas	Mal manejo de las Base de Datos	s	Políticas y normas Institucionales	m
	Robo	Divulgación de información.	s	controles lógicos.	m
	Robo por uso de laptops	Divulgación de información.	s	Políticas militares	m
	Sabotaje	Pérdida o modificación de datos,pérdida de tiempo y productividad.	s	Backups y controles físicos y lógicos.	e
	Seguridad de base de datos deficiente	Modificación de información sin autorización	s	Políticas y normas Institucionales	m
	Spoofing y sniffing	Divulgación y modificación de información.	n		d
	Transferencia de datos incorrectos	Inconsistencia de datos.	s	Controles lógicos.	e
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Software de aplicación, programas fuente, sistemas operativos	Acceso no autorizado a datos (borrado,modificación, etc.)	Modificación del software en desarrollo.	s	Controles físicos y controles de accesos lógicos a desarrollo de software.	m
	Aplicaciones sin licencia	Multas y problemas con Software Legal.	s	Software de auditoría (Antiris)	m
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de software de aplicación y sistemas operativos	n		
	Conocimiento insuficiente de los requerimientos en el desarrollo de sistemas	Sistema inestable y excesivos pedidos de cambios.	s	Metodología de análisis y diseño estructurada.	m
	Error de configuración	Mal funcionamiento de los sistemas.	s	Existen herramientas de análisis.	e
	Errores en las funciones de encriptación	Problemas en la recuperación de archivos encriptados o divulgación de información.	s	Personal especializado.	e
	Falla del sistema	Falta de sistema y posibles demoras.	s	Backup y sistemas de respaldo.	m
	Falta de confidencialidad	Divulgación de información.	s	controles lógicos.	e
	Fraude	Modificación del software en desarrollo.	s	Controles físicos y controles de accesos lógicos a desarrollo de software.	m
	Incendios	Pérdida de programas	s	políticas y normas Institucionales	m
	Mala administración de control de acceso	Divulgación y modificación de información.	s	Controles de acceso lógico, reforzados en datos críticos.	e
	Pérdida de datos	Divulgación de información.	s	Backup de respaldo.	e
	Poca adaptación a cambios	Sistema inestable y de difícil modificación.	s	Metodología de análisis y diseño estructurada.	e
	Prueba de software deficiente	Sistema poco confiable.	s	Metodología de análisis y diseño estructurada.	e
	Reglas insuficientes o ausencia de ellas	Mal manejo de aplicaciones	n		
	Robo de información	Pérdida de programas	s	Controles físicos	m
	Software desactualizado	Probabilidad incremental de vulnerabilidades y virus.	s	Mantenimiento por departamento técnico y constante evaluación de las aplicaciones.	m
	Virus	Inestabilidad y mal funcionamiento de sistemas.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Backup (respaldos de hardware, software y datos)	Copia no autorizada a un medio de datos	Robo de información.	s	Controles de seguridad física en el ingreso al centro de cómputos y controles de acceso lógicos al servidor.	m
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de Backups	n		d
	Falla en medios externos	Pérdida de backups.	n		d
	Falta de espacio de almacenamiento	Falla en la generación del backup.	s	Capacidad de almacenamiento suficiente	e
	Fraude	Modificación o pérdida de Backup	s	Controles físicos	m
	Incendios	Pérdida de información	s	extintores, políticas y normas internas	m
	Mala configuración de las tareas programadas de backups	Falta de copias de respaldo de datos.	s	Agenda de backups eficiente.	e
	Mala integridad de los datos resguardados.	Errores durante la restauración de datos.	n		d
	Medios de datos no están disponibles cuando son necesarios	Pérdida de backup y retraso del sistema.	s	Numerosas copias de respaldo por posibles errores.	e
	Pérdida de backups	Falta de datos, incapacidad de restaurarlos y divulgación de información.	n		d
	Reglas insuficientes o ausencia de ellas	Mal manejo de Backups	n		d
	Robo	Incapacidad de restaurarlos y divulgación de información.	s	Controles de acceso físicos, guardia militar, alarmas, sistema de camaras.	e
	Rótulos inadecuado en los medios de datos	Errores durante la restauración de datos.	s	Rótulos capaces de diferenciar cada medio de datos como único.	e
	Sabotaje	Pérdida o robo de información.	s	Controles de acceso físicos, guardia militar y copias de respaldo.	e
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Virus	Pérdida de datos de backup.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Datos en transito, datos de configuración, datos en medios externos	Copia no autorizada a un medio de datos	Robo de información.	s	Controles de seguridad física, controles de acceso lógicos a los sistemas.	m
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de datos (transito, configuración, medios externos)	n		d
	Errores en las funciones de encriptación	Divulgación de información (passwords)	s	Control en la configuración de la red.	e
	Falla en medios externos	Pérdida de datos en medios externos.	s	Recuperación de información almacenada	e
	Mala integridad de los datos	Inconsistencia de información.	s	Controles de integridad en la transmisión, en el ingreso de datos.	e
	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo y productividad por falta de datos.	s	Backup de medios de datos	e
	Modificación e intercepción de datos en tránsito	Divulgación de información	s	Controles de acceso lógico y físico	m
	Pérdida de confidencialidad en datos privados y de sistema	Divulgación de información.	s	Controles de acceso lógico y físico a los medios de almacenamiento de datos, reforzados en datos críticos.	m
	Pérdida de datos en tránsito	Divulgación de información.	s	Control en la configuración de la red.	m
	Portapapeles, impresoras o directorios compartidos	Divulgación o robo de información.	s	Prohibición de servicios mediante acceso lógico	e
	Robo de información	Divulgación y pérdida de información	s	Controles físicos	m
	Robo por uso de laptops	Divulgación o robo de información.	s	Políticas internas militares.	e
	Sabotaje	Pérdida o robo de información.	s	Control en la configuración de la red y acceso lógico	m
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m e)
Administradores (Centros Tecnológicos)	Administración impropia del sistema de IT (responsabilidades y roles del personal de sistemas)	Asignación de responsabilidades impropia.	s	Políticas y normas militares	m
	Almacenamiento de contraseñas negligente	Divulgación de password y uso indebido de derechos de usuarios.	s	Administración de acceso lógico por software de aplicación	m
	Configuración impropia del servicio de Mail	Divulgación de mensajes, uso del servidor para enviar SPAM.	s	La configuración del Mail la realiza y mantiene el departamento técnico.	e
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de los Centros Tecnológicos	n		d
	Deficiencias conceptuales en la red	Mala configuración de la red	s	Capacitación del Administrador	m
	Errores de configuración y operación del sistema.	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades.	s	El mantenimiento diario lo realiza el departamento técnico.	e
	Falta de auditorías en sistema operativo	Imposibilidad del seguimiento de usuarios y de la generación de reportes.	s	Existen logs generados automáticamente por el sistema operativo y por sus aplicaciones principales.	e
	Fraude	Modificación o pérdida de información	s	Políticas y normas militares	m
	Mala evaluación de datos de auditoría	No se analizan los logs y por lo tanto no hay evaluación de los resultados.	n		d
	Mal uso de derechos de administrador	Mala distribución de los permisos y de las cuentas de administrador.	s	Políticas y normas militares	d
	Penetración, intercepción o manipulación de líneas de comunicación	Divulgación de información	n		d
	Reglas insuficientes o ausencia de ellas	Mal manejo de los Centros Tecnológicos	n		d
	Uso de derechos sin autorización	Mal manejo de los Centros Tecnológicos	s	Políticas, éticas y normas internas	m
	Uso impropio del sistema de Tecnologías de la Información	Mal manejo de los sistemas de Tecnología de Información	n	Políticas y normas internas	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Cableado, antenas, switches, hubs, modems, routers, firewalls	Ancho de banda insuficiente	Transmisión pesada en la red o imposibilidad de utilizar el sistema online.	s	Recursos en ancho de banda y control de tráfico en la red	m
	Conexión de cables inadmisible	Pinchaduras de cables, robo de datos, spoofing y sniffing.	n		d
	Daño o destrucción de cables o equipamiento inadvertido	Pinchaduras de cables, robo de datos, spoofing y sniffing.	n		d
	Deficiencias conceptuales en la red	Mala configuración de los equipos de la red	s	Manuales de configuración de la red	m
	Factores ambientales	Interferencias o daños de equipamiento.	s	Utilización de UPS	m
	Incendios	Pérdida de los equipos	s	extintores, políticas y normas de seguridad	m
	Interferencias	Errores en los datos de transmisión o imposibilidad de utilizar el sistema online.	s	Estructura del cableado sin fallas	m
	Límite de vida útil de equipos.	Equipos obsoletos e imposibilidad de utilizar el sistema.	s	Equipamiento actualizado y mantenimiento del cableado.	m
	Longitud de los cables de red excedida	Transmisión lenta o con interferencias, o imposibilidad de utilizar el sistema on-line.	s	Mantenimiento del cableado.	m
	Mal mantenimiento	Errores de transmisión o interrupción del servicio de red.	s	Mantenimiento por el Departamento Técnico.	e
	Reducción de velocidad de transmisión	Pérdida de tiempo de los usuarios, o imposibilidad de utilizar el sistema online.	s	Recursos abundantes en ancho de banda y control de tráfico en la red	e
	Riesgo por el personal de limpieza o personal externo	Daño en cables o equipos, interrupción del sistema on-line.	s	Mantenimiento del departamento Técnico	d

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Red	Abuso de puertos para el mantenimiento remoto	Posibles intrusiones y robo o divulgación de información.	s	Política de configuración de puertos restringida y herramientas de monitoreo de puertos.	m
	Ausencia o falta de segmentación	Tramos de red extensos y dificultades en la comunicación.	s	Red segmentada física y lógicamente por sectores.	e
	Complejidad en el diseño de las redes de sistemas de IT	Dificultad en la administración y en el mantenimiento.	s	Diseño de red simple con topología de bus y estrella.	e
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de la red	n		d
	Utilización de cuentas de usuarios sin autorización	Intrusión de usuarios no autorizados al sistema.	s	Mediante el bloqueo de cuentas del Sistema Operativo y herramienta de control acceso lógico	d
	Configuración inadecuada de componentes de red	Errores de transmisión, interrupción del servicio de red.	s	Equipamiento de red configurado por departamento técnico.	e
	Deficiencias conceptuales en la red	Mal manejo de la red	s	Capacitación al personal	m
	Denegación de Servicio	Interrupción de todos o algunos de los servicios de red.	s	Mediante herramienta de control de acceso lógico	m
	Errores de configuración y operación	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades.	s	Control regular por departamento Técnico	e
	Falla en la LAN y WAN	Una o más sucursales incomunicadas.	s	Mediante canal de datos de respaldos	m
	Falta de autenticación	Posibles intrusiones y robo o divulgación de información.	s	Controles de acceso a datos y a equipos, y firewall.	m
	Mal uso de servicios de mail	Disminución de la performance del ancho de banda	s	Control en los mensajes de mail enviados	m
	Reglas insuficientes o ausencia de ellas	Mal manejo de la red	n		d
	Penetración, intercepción o manipulación de líneas de comunicación	Divulgación de información.	s	Controles de acceso lógicos	m
	Sincronización de tiempo inadecuada	Inconsistencia en datos.	s	Actualización de la base de datos.	e
	Spoofing y sniffing	Divulgación, modificación y robo de información	n		d
	Transporte inseguro de archivos	Divulgación de información.	s	Política y normas militares	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Usuarios	Acceso no autorizado a datos	Divulgación o robo de información.	s	Controles de acceso lógico a datos en las aplicaciones.	m
	Borrado, modificación o revelación desautorizada o inadvertida de información	Inconsistencia de datos o datos faltantes.	s	Controles lógicos a datos.	m
	Condiciones de trabajo adversas	Predisposición a distracción, bajo rendimiento de usuarios.	s	Ambiente de trabajo cómodo.	m
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de la información	n		d
	Destrucción de un componente de hardware	Pérdida de tiempo por necesidad de reemplazo.	s	Backup de hardware	m
	Destrucción negligente de datos	Pérdida de información.	s	Controles lógicos a datos en las aplicaciones, Políticas y normas militares	m
	Documentación deficiente	Mayor probabilidad de errores por falta de instrucciones.	n		d
	Entrada sin autorización a departamentos y cubículos	Robo de equipos o insumos, divulgación de datos.	s	Control de acceso físico a instalaciones del centro de cómputos.	m
	Entrenamiento de usuarios inadecuado	Predisposición a errores y bajo rendimiento de usuarios.	n		d
	Falta de auditorías	Predisposición a un rendimiento mediocre y falta de concienciación sobre responsabilidades y seguridad.	n		d
	Falta de cuidado en el manejo de la información (Ej. Password)	Divulgación de datos.	s	Insistencia con respecto al uso discreto de datos críticos.	m
	Mal uso de derechos de administrador (sesiones abiertas)	Divulgación o robo de información,sabotaje interno.	s	Políticas, normas y éticas militares	d
	No-cumplimiento con las medidas de seguridad del sistema	Medidas correctivas tomadas por la gerencia, según la gravedad del incidente.	n		m
	Penetración, intercepción o manipulación de líneas de comunicación	Divulgación de la información	s	controles de acceso lógico	m
	Pérdida de confidencialidad o integridad de datos como resultado de un error humano.	Error en la información.	s	Controles lógicos de acceso a datos y de integridad de datos de entrada al sistema.	e
	Desvinculación del personal	Robo o modificación de información,sabotaje interno.	s	Políticas, normas internas	m
	Reglas insuficientes o ausencia de ellas	Mal manejo de la información	n		d
	Uso de derechos sin autorización	Mal manejo de la información	s	Políticas y normas internas	m
	Uso impropio del sistema de Tecnologías de la Información	Mal manejo de la información	s	Políticas	m
	Uso descontrolado de recursos (DoS)	Retraso en las actividades o falta de sistema.	n		d

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	Acceso no autorizado a datos de documentación.	Divulgación, robo o modificación de información.	s	Control de acceso físico a instalaciones del centro de cómputos.	m
	Borrado, modificación o revelación desautorizada de información	Documentación incorrecta.	s	Normas y Políticas Institucionales	m
	Visualización de información	Divulgación de información.	s	Controles de acceso lógico al sistema.	e
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de la información	n		d
	Copia no autorizada a un medio de datos	Divulgación de información.	s	Control de acceso físico a instalaciones del centro de cómputos.	m
	Descripción de archivos inadecuada	Documentación incorrecta.	n		d
	Destrucción negligente de datos	Documentación incorrecta.	s	Políticas y normas internas	m
	Documentación insuficiente o faltante, funciones no documentadas	Entorpecimiento de la administración y uso del sistema.	n		d
	Factores ambientales	Destrucción de datos.	s	Seguridad física	m
	Fraude	Modificación de información	n		
	Incendios	Pérdida dela información	s	extintores, políticas de seguridad	m
	Mal interpretación	Entorpecimiento de la administración y uso del sistema.	n		d
	Mantenimiento inadecuado o ausente	Documentación incorrecta, redundante y compleja	n		d
	Medios de datos no están disponibles cuando son necesarios	Entorpecimiento de la administración y uso del sistema.	n		d
	Reglas insuficientes o ausencia de ellas	Mal manejo de la información	n		d
	Robo	Divulgación de información.	s	Controles de acceso físico a datos.	m
	Uso sin autorización	Divulgación, robo o modificación de información.	s	Controles de acceso físico a datos.	m
	Virus, gusanos y caballos de Troya	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	Corte de luz, UPS descargado o variaciones de voltaje.	Interrupción del funcionamiento de equipos.	s	Generador, UPS, estabilizador	e
	Destrucción o mal funcionamiento de un componente	Interrupción de la tarea del usuario.	s	Insumos de respaldo y equipamiento asegurado.	e
	Factores ambientales	Destrucción o avería de equipos.	s	Insumos de respaldo y equipamiento asegurado.	e
	Incendios	Pérdida de la información	s	Políticas de seguridad, extintores	m
	Límite de vida útil	Avería de equipos.	s	Insumos de respaldo y equipamiento asegurado.	e
	Mal mantenimiento	Avería de equipos e incremento en el costo de equipamiento de respaldo.	s	Mantenimiento por departamento técnico.	e
	Robo	Pérdida de equipamiento e interrupción de la tarea del usuario.	s	Controles de acceso físicos, guardias militares, sistemas de camaras, alarmas.	e

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	Factores ambientales	Destrucción de insumos.	s	Insumos de respaldo.	e
	Incendios	Pérdida de la información	s	políticas de seguridad, extintores	m
	Límite de vida útil	Destrucción o avería de insumos.	s	Insumos de respaldo.	e
	Recursos escasos.	Interrupción en el funcionamiento normal de la empresa.	s	Insumos de respaldo.	e
	Uso descontrolado de recursos.	Incremento no justificado del gasto de insumos.	s	Administración de insumos.	e
	Robo	Pérdida de insumos e incremento en el gasto.	s	Controles de acceso físicos, guardias militares,sistemas de camaras	e
	Transporte inseguro de medios de datos	Pérdida de datos, de insumos, e incremento en el gasto.	s	Personal asignado a dicha tarea con normas	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva? (d-m-e)
Datos de Usuarios	Falta de espacio de almacenamiento	Retraso de las actividades.	s	Capacidad de almacenamiento sobredimensionada.	e
	Conocimiento insuficiente de los documentos Institucionales	Mal manejo de la información	n		d
	Mala configuración de las tareas programadas de backups	Pérdida de datos del usuario.	s	Control por medio del Departamento Técnico	m
	Medios de datos no están disponibles cuando son necesarios	Retraso en las actividades.	s	Permanente disponibilidad de estos medios por personal del centro de cómputos.	e
	Pérdida de backups	Pérdida de datos del usuario y retraso de la tarea.	s	Controles de acceso físico y lógico al equipo usado para tal copias de respaldo.	m
	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información.	s	Controles de acceso físico y lógico a las PC´s de los usuarios.	m
	Portapapeles, impresoras o directorios compartidos	Divulgación de información.	s	Carpetas de usuarios no compartidas en la red.	e
	Reglas insuficientes o ausencia de ellas	Mal manejo de la información	n		d
	Robo	Divulgación de información.	s	Controles de acceso físico y lógico a los equipos	e
	Sabotaje	Pérdida, modificación o divulgación de datos.	s	Controles de acceso físico y lógico a los equipos y copias de respaldo de los datos	e
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

3.1.4.4.- Cálculos de los niveles de vulnerabilidad

Para la elaboración de la tabla siguiente se utilizó la lista de factores de riesgos y su probabilidad de ocurrencia (Escala 1-3) con respecto a los activos Institucionales relacionados con su nivel de importancia (Escala 1-10), para así determinar el porcentaje de probabilidad de que un riesgo ocurra en razón a todos los posibles riesgos que afectan al activo.

$$\%\,prob.riesgos = \frac{probabilidad\_de\_ocurrencia \times 100}{cantidad\_de\_factores\_de\_riesgos}$$

Es decir, aplicado al primer factor de riesgo *acceso no autorizado* que interviene en el activo *Servidores* se calcula el porcentaje de probabilidad de riesgos de la siguiente manera:

$$\%\,prob.riesgos = \frac{2 \times 100}{13} = 15.38$$

De igual manera, basados en el mismo factor de riesgo se calculará el nivel de vulnerabilidad que tiene el activo *servidores* con respecto al factor de riesgo *acceso no autorizado* identificando el nivel de importancia del activo, que en este caso corresponde a *10.*

$$Nivel\_de\_vulnerabilidad = \left(\%prob.riesgos \times nivel\_de\_importancia\right)^{15}$$

$$Nivel\_de\_vulnerabilidad = \left(15.38 \times 10\right) = 153.85$$

[15] www.segu-info.com.ar - Seguridad Informática/Evaluación de Riesgos

Aplicación de la Tabla 2.3: (Cálculo de niveles de probabilidad)

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
1	Servidores	10	Acceso no autorizado	2	15,38	153,85
			Corte de luz, UPS descargado o variaciones de voltaje.	1	7,69	76,92
			Deficiencias conceptuales en la red	1	7,69	76,92
			Destrucción de un componente	1	7,69	76,92
			Error de configuración	1	7,69	76,92
			Factores ambientales	1	7,69	76,92
			Incendios	3	23,08	230,77
			Límite de vida útil - Máquinas obsoletas	1	7,69	76,92
			Mal mantenimiento	1	7,69	76,92
			Modificación no autorizada de datos	1	7,69	76,92
			Robo	1	7,69	76,92
			Robo de información	1	7,69	76,92
			Virus	3	23,08	230,77
Cantidades de factores de riesgos =				13		**1384,62**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
2	Bases de datos	10	Copia no autorizada a un medio de datos	2	9,09	90,91
			Conocimiento insuficiente de los documentos Institucionales	2	9,09	90,91
			Falla de base de datos	1	4,55	45,45
			Falla en medios externos	1	4,55	45,45
			Falta de espacio de almacenamiento	1	4,55	45,45
			Fraude	2	9,09	90,91
			Incendios	3	13,64	136,36
			Mala configuración de las tareas programadas de backups	1	4,55	45,45
			Mala integridad de los datos	1	4,55	45,45
			Medios de datos no están disponibles cuando son necesarios	1	4,55	45,45
			Pérdida de backups	2	9,09	90,91
			Pérdida de confidencialidad en datos privados y de sistema	1	4,55	45,45
			Pérdida de datos en tránsito	1	4,55	45,45
			Portapapeles, impresoras o directorios compartidos	1	4,55	45,45
			Reglas insuficientes o ausencia de ellas	2	9,09	90,91
			Robo	1	4,55	45,45
			Robo por uso de laptops	1	4,55	45,45
			Sabotaje	1	4,55	45,45
			Seguridad de base de datos deficiente	1	4,55	45,45
			Spoofing y sniffing	1	4,55	45,45
			Transferencia de datos incorrectos	1	4,55	45,45
			Virus	3	13,64	136,36
			Cantidades de factores de riesgos =	22		**1409,09**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
3	Software de aplicación, programas fuente, sistemas operativos	9	Acceso no autorizado a datos (borrado,modificación, etc.)	2	11,11	100,00
			Aplicaciones sin licencia	2	11,11	100,00
			Conocimiento insuficiente de los documentos Institucionales	2	11,11	100,00
			Conocimiento insuficiente de los requerimientos en el desarrollo de sistemas	3	16,67	150,00
			Error de configuración	1	5,56	50,00
			Errores en las funciones de encriptación	1	5,56	50,00
			Falla del sistema	1	5,56	50,00
			Falta de confidencialidad	1	5,56	50,00
			Fraude	2	11,11	100,00
			Incendios	3	16,67	150,00
			Mala administración de control de acceso	1	5,56	50,00
			Pérdida de datos	1	5,56	50,00
			Poca adaptación a cambios	1	5,56	50,00
			Prueba de software deficiente	1	5,56	50,00
			Reglas insuficientes o ausencia de ellas	2	11,11	100,00
			Robo de información	1	5,56	50,00
			Software desactualizado	1	5,56	50,00
			Virus	3	16,67	150,00
			Cantidades de factores de riesgos =	18		**1450,00**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
4	Backup (respaldos de hardware, software y datos)	9	Copia no autorizada a un medio de datos	2	12,50	112,5
			Conocimiento insuficiente de los documentos Institucionales	2	12,50	112,5
			Falla en medios externos	1	6,25	56,25
			Falta de espacio de almacenamiento	1	6,25	56,25
			Fraude	2	12,50	112,5
			Incendios	3	18,75	168,75
			Mala configuración de las tareas programadas de backups	1	6,25	56,25
			Mala integridad de los datos resguardados.	1	6,25	56,25
			Medios de datos no están disponibles cuando son necesarios	1	6,25	56,25
			Pérdida de backups	2	12,50	112,5
			Reglas insuficientes o ausencia de ellas	2	12,50	112,5
			Robo	1	6,25	56,25
			Rótulos inadecuado en los medios de datos	1	6,25	56,25
			Sabotaje	1	6,25	56,25
			Spoofing y sniffing	1	6,25	56,25
			Virus	2	12,50	112,5
			Cantidades de factores de riesgos =	16		**1350**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
5	Datos en transito, datos de configuración, datos en medios externos	8	Copia no autorizada a un medio de datos	2	13,33	106,67
			Conocimiento insuficiente de los documentos Institucionales	2	13,33	106,67
			Errores en las funciones de encriptación	1	6,67	53,33
			Falla en medios externos	1	6,67	53,33
			Mala integridad de los datos	1	6,67	53,33
			Medios de datos no están disponibles cuando son necesarios	1	6,67	53,33
			Modificación e intercepción de datos en tránsito	1	6,67	53,33
			Perdida de confidencialidad en datos privados y de sistema	1	6,67	53,33
			Perdida de datos en tránsito	1	6,67	53,33
			Portapapeles, impresoras o directorios compartidos	1	6,67	53,33
			Robo de información	1	6,67	53,33
			Robo por uso de laptops	1	6,67	53,33
			Sabotaje	1	6,67	53,33
			Spoofing y sniffing	1	6,67	53,33
			Virus	3	20,00	160,00
			Cantidades de factores de riesgos =	15		**1013,33**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
6	Administradores (Centros Tecnológicos)	7	Administración impropia del sistema de IT (responsabilidades y roles del personal de sistemas)	1	7,14	50
			Almacenamiento de passwords negligente	2	14,29	100
			Configuración impropia del servicio de Mail	2	14,29	100
			Conocimiento insuficiente de los documentos Institucionales	2	14,29	100
			Deficiencias conceptuales en la red	1	7,14	50
			Errores de configuración y operación del sistema.	1	7,14	50
			Falta de auditorías en sistema operativo	3	21,43	150
			Fraude	2	14,29	100
			Mala evaluación de datos de auditoría	3	21,43	150
			Penetración, intercepción o manipulación de líneas de comunicación	1	7,14	50
			Reglas insuficientes o ausencia de ellas	2	14,29	100
			Uso de derechos sin autorización	2	14,29	100
			Uso impropio del sistema de Tecnologías de la Información	1	7,14	50
			Mal uso de derechos de administrador	3	21,43	150
			Cantidades de factores de riesgos =	14		**1300**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
7	Cableado, antenas, switches, hubs, modems, routers, firewalls	6	Ancho de banda insuficiente	1	8,33	50
			Conexión de cables inadmisible	1	8,33	50
			Daño o destrucción de cables o equipamiento inadvertido	1	8,33	50
			Deficiencias conceptuales en la red	1	8,33	50
			Factores ambientales	1	8,33	50
			Incendios	3	25,00	150
			Interferencias	1	8,33	50
			Límite de vida útil de equipos.	1	8,33	50
			Longitud de los cables de red excedida	1	8,33	50
			Mal mantenimiento	1	8,33	50
			Reducción de velocidad de transmisión	1	8,33	50
			Riesgo por el personal de limpieza o personal externo	1	8,33	50
			Cantidades de factores de riesgos =	12		**700**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
8	Red	6	Abuso de puertos para el mantenimiento remoto	1	5,88	35,29
			Ausencia o falta de segmentación	2	11,76	70,59
			Complejidad en el diseño de las redes de sistemas de IT	1	5,88	35,29
			Conocimiento insuficiente de los documentos Institucionales	2	11,76	70,59
			Utilización de cuentas de usuarios sin autorización	2	11,76	70,59
			Configuración inadecuada de componentes de red	2	11,76	70,59
			Deficiencias conceptuales en la red	1	5,88	35,29
			Denegación de Servicio	1	5,88	35,29
			Errores de configuración y operación	1	5,88	35,29
			Falla en la LAN y WAN	1	5,88	35,29
			Falta de autenticación	1	5,88	35,29
			Mal uso de servicios de mail	2	11,76	70,59
			Reglas insuficientes o ausencia de ellas	2	11,76	70,59
			Penetración, intercepción o manipulación de líneas de comunicación	1	5,88	35,29
			Sincronización de tiempo inadecuada	1	5,88	35,29
			Spoofing y sniffing	1	5,88	35,29
			Transporte inseguro de archivos	1	5,88	35,29
			Cantidades de factores de riesgos =	17		**811,76**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
9	Usuarios	5	Acceso no autorizado a datos	2	10,00	50,00
			Borrado, modificación o revelación desautorizada o inadvertida de información	1	5,00	25,00
			Condiciones de trabajo adversas	1	5,00	25,00
			Conocimiento insuficiente de los documentos Institucionales	2	10,00	50,00
			Destrucción de un componente de hardware	1	5,00	25,00
			Destrucción negligente de datos	1	5,00	25,00
			Documentación deficiente	3	15,00	75,00
			Entrada sin autorización a departamentos y cubículos	2	10,00	50,00
			Entrenamiento de usuarios inadecuado	2	10,00	50,00
			Falta de auditorías	3	15,00	75,00
			Falta de cuidado en el manejo de la información (Ej. Password)	2	10,00	50,00
			Mal uso de derechos de administrador (sesiones abiertas)	3	15,00	75,00
			No-cumplimiento con las medidas de seguridad del sistema	2	10,00	50,00
			Penetración, intercepción o manipulación de líneas de comunicación	1	5,00	25,00
			Pérdida de confidencialidad o integridad de datos como resultado de un error humano.	1	5,00	25,00
			Reglas insuficientes o ausencia de ellas	2	10,00	50,00
			Desvinculación del personal	1	5,00	25,00
			Uso de derechos sin autorización	2	10,00	50,00
			Uso impropio del sistema de Tecnologías de la Información	1	5,00	25,00
			Uso descontrolado de recursos (DoS)	1	5,00	25,00
			Cantidades de factores de riesgos =	20		**850,00**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
10	Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4	Acceso no autorizado a datos de documentación.	2	11,11	44,44
			Borrado, modificación o revelación desautorizada de información	1	5,56	22,22
			Conocimiento insuficiente de los documentos Institucionales	2	11,11	44,44
			Visualización de información	1	5,56	22,22
			Copia no autorizada a un medio de datos	2	11,11	44,44
			Descripción de archivos inadecuada	1	5,56	22,22
			Destrucción negligente de datos	1	5,56	22,22
			Documentación insuficiente o faltante, funciones no documentadas	3	16,67	66,67
			Factores ambientales	1	5,56	22,22
			Fraude	2	11,11	44,44
			Incendios	3	16,67	66,67
			Mal interpretación	2	11,11	44,44
			Mantenimiento inadecuado o ausente	2	11,11	44,44
			Medios de datos no están disponibles cuando son necesarios	1	5,56	22,22
			Reglas insuficientes o ausencia de ellas	2	11,11	44,44
			Robo	1	5,56	22,22
			Uso sin autorización	1	5,56	22,22
			Virus, gusanos y caballos de Troya	3	16,67	66,67
			Cantidades de factores de riesgos =	18		**688,89**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
11	Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	3	Corte de luz, UPS descargado o variaciones de voltaje.	1	14,29	42,86
			Destrucción o mal funcionamiento de un componente	1	14,29	42,86
			Factores ambientales	1	14,29	42,86
			Incendios	3	42,86	128,57
			Límite de vida útil	1	14,29	42,86
			Mal mantenimiento	1	14,29	42,86
			Robo	1	14,29	42,86
			Cantidades de factores de riesgos =	7		**385,71**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
12	Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	2	Factores ambientales	1	14,29	28,57
			Incendios	3	42,86	85,71
			Límite de vida útil	1	14,29	28,57
			Recursos escasos.	1	14,29	28,57
			Uso descontrolado de recursos.	1	14,29	28,57
			Robo	1	14,29	28,57
			Transporte inseguro de medios de datos	1	14,29	28,57
			Cantidades de factores de riesgos =	7		**257,14**

N"Activo	Nombre del Activo	Nivel de Importancia (1-10)	Factor de Riesgo	Probabilidad de Ocurrencia (1-3)	%Prob.riesgos	Nivel de vulnerabilidad
13	Datos de usuarios	1	Falta de espacio de almacenamiento	1	8,33	8,33
			Conocimiento insuficiente de los documentos Institucionales	2	16,67	16,67
			Mala configuración de las tareas programadas de backups	1	8,33	8,33
			Medios de datos no están disponibles cuando son necesarios	1	8,33	8,33
			Pérdida de backups	1	8,33	8,33
			Perdida de confidencialidad en datos privados y de sistema	1	8,33	8,33
			Portapapeles, impresoras o directorios compartidos	1	8,33	8,33
			Reglas insuficientes o ausencia de ellas	2	16,67	16,67
			Robo	1	8,33	8,33
			Sabotaje	1	8,33	8,33
			Spoofing y sniffing	1	8,33	8,33
			Virus	3	25,00	25,00
			Cantidades de factores de riesgos =	12		**133,33**

3.1.4.5.- Cálculo de Porcentaje de riesgo

Para la elaboración de la tabla siguiente se utilizó el Nivel de Vulnerabilidad total de cada activo respecto a sus factores de riesgos relacionados con la importancia que tiene cada activo. Los niveles de vulnerabilidad serán expresados en tres escalas de importancia: Escala 1-10, Escala 1-3 y escala a 1-1. La relación que tiene cada escala se resume en la siguiente tabla la que indicará cual es la equivalencia que tiene un determinado activo en las tres escalas.

Tabla 3.3: (Escala de Importancias)

Activo	**Importancia Escala (1-10)**	**Importancia Escala (1-3)**	**Importancia Escala (1-1)**
Servidores	10	3	1
Bases de datos	10	3	1
Software de aplicación, programas fuente, sistemas operativos	9	3	1
Backup (respaldos de hardware, software y datos)	9	3	1
Datos en transito, datos de configuración, datos en medios externos	8	3	1
Administradores (Centros Tecnológicos)	7	3	1
Cableado, antenas, switches, hubs, modems, routers, firewalls	6	2	1
Red	6	2	
Usuarios	5	2	1
Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4	2	1
Hardware (teclado, monitor, unidades de discos,	3	1	1

medios removibles,etc.)			
Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	2	1	1
Datos de usuarios	1	1	1

Una vez identificadas las escalas de importancia se debe determinar el nivel de vulnerabilidad así como el porcentaje de riesgo que tiene cada activo.

Para la vulnerabilidad en escala 1-10 se tomar el total del nivel de vulnerabilidad de cada activo de las tablas anteriores, sumar todos los valores y obtener el valor total de riesgos encontrados en la escala 1-10 de importancia (***imp (1-10***)). Una vez obtenido el valor total se debe obtener el porcentaje de riesgo que tiene cada activo mediante la siguiente fórmula:

$$R\% = \frac{imp(1-10)*100}{\sum imp(1-10)}$$

Aplicado al activo *Datos de usuario* el porcentaje de riesgos es en escala 1-10:

$$R\% = \frac{133.33*100}{11733.87} = 1.14\%$$

Para obtener el nivel de vulnerabilidad en escala 1-3 se necesita realizar una transformación de los valores obtenidos en la escala 1-10 para lo cual se sigue la siguiente fórmula en la que intervienen las escalas antes mostradas:

$$imp(1-3) = \frac{imp(1-10)*Escala(1-3)}{Escala(1-10)}$$

Aplicado al activo *Software de Aplicación* el nivel de vulnerabilidad en escala 1-3 es*:*

$$imp(1-3) = \frac{1450*3}{9} = 483.33$$

De igual manera calculamos el porcentaje de riesgo que tiene el activo de acuerdo al nivel de vulnerabilidad encontrado en escala 1-3

$$R\% = \frac{imp(1-3)*100}{\sum imp(1-3)}$$

Aplicado al activo *Software de Aplicación* el porcentaje de riesgos en escala 1-3 es:

$$R\% = \frac{483.33*100}{4287.42} = 11.27\%$$

Y para finalizar obtenemos el nivel de vulnerabilidad en escala 1-1 para ello se necesita realizar una transformación de los valores obtenidos en la escala 1-10 para lo cual se sigue la siguiente fórmula en la que intervienen las escalas antes mostradas:

$$imp(1-1) = \frac{imp(1-10)*Escala(1-1)}{Escal(1-10)}$$

Aplicado al activo *Software de Aplicación* el nivel de vulnerabilidad en escala 1-1 es:

$$imp(1-1) = \frac{1450*1}{9} = 161.11$$

Una vez calculado la vulnerabilidad del activo de acuerdo a su importancia el porcentaje de riesgo en escala 1-1 es el siguiente:

$$R\% = \frac{imp(1-1)*100}{\sum imp(1-1)}$$

Aplicado al activo *Software de Aplicación* el porcentaje de riesgos en escala 1-1 es:

$$R\% = \frac{161.11*100}{1887.52} = 8.54\%$$

Aplicación de la Tabla 2.4: (Niveles de Vulnerabilidad)

Activos	Niveles de Vulnerabilidad					
	Imp (1 - 10)	R %	Imp (1 - 3)	R %	Imp (1-1)	R %
1 Datos de usuarios	133,33	1,14	133,33	3,11	133,33	7,06
2 Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	257,14	2,19	128,57	3,00	128,57	6,81
3 Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	385,71	3,29	128,57	3,00	128,57	6,81
4 Cableado, antenas, switches, hubs, modems, routers, firewalls	700	5,97	233,33	5,44	116,67	6,18
5 Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	688,89	5,87	344,45	8,03	172,22	9,12
6 Usuarios	850	7,24	340,00	7,93	170,00	9,01
7 Red	811,76	6,92	270,59	6,31	135,29	7,17
8 Datos en transito, datos de configuración, datos en medios externos	1013,33	8,64	380,00	8,86	126,67	6,71
9 Backup (respaldos de hardware, software y datos)	1350	11,51	450,00	10,50	150,00	7,95
10 Bases de datos	1409,09	12,01	422,73	9,86	140,91	7,47
11 Servidores	1384,62	11,80	415,39	9,69	138,46	7,34
12 Software de aplicación, programas fuente, sistemas operativos	1450	12,36	483,33	11,27	161,11	8,54
13 Administradores (Centros Tecnológicos)	1300	11,08	557,14	12,99	185,71	9,84
	11733,87	**100,00**	**4287,4229**	**100,00**	**1887,52**	**100,00**

3.1.4.6.- Nivel de Importancia de los activos

El objetivo de determinar la siguiente tabla es de verificar si la importancia actual asignada a un activo es el ideal de acuerdo al nivel de riesgos al que está expuesto el activo después del análisis correspondiente en las tablas anteriores.

Debido a que la importancia especificada a los activos está en una escala 1-10 se necesitará el nivel de vulnerabilidad en esta escala así como su porcentaje de riesgos y el correspondiente valor de importancia de cada activo con su respectivo porcentaje

Para obtener la diferencia de porcentajes (***Dif de %***) se debe restar el porcentaje del nivel de vulnerabilidad con el porcentaje de la importancia actual de cada activo, es decir:

$$Dif\_de\_\% = \%\_Nivel\_de\_Vulnerabilidad - \%\_de\_importancia\_actual$$

Aplicado al activo *Datos de usuario* la diferencia de porcentaje es:

$$Dif\ \_\ de\ \_\ \% = 1.13 - 1.25 = -0.11$$

Es importante destacar que el valor negativo (-) implica que el activo está sobrevaluado en el valor asignado de la importancia y el signo positivo (+) que el activo está menospreciado.

Para calcular la Diferencia de importancia (***Dif de Imp***) se debe multiplicar la importancia actual, la Diferencia de porcentajes y a esto por 10 y divido para el 100 %. La razón de multiplicar por el valor de 10 y dividir para el 100 % es la de obtener los datos en

la escala 1-10 y no tener los datos en términos porcentuales, esto es con el objetivo de poder la importancia ideal que debe tener el activo.

$$Dif\_de\_imp = \frac{importancia\_actual * Dif\_de\_\% * 10}{100\%}$$

.

Aplicado al activo *Datos de Usuario* la diferencia de importancias es:

$$Dif\ \_de\_imp = \frac{1 * -0.11 * 10}{100\%} = -0.01$$

Una vez calculado la diferencia de importancia calculamos la ***importancia ideal*** que debe ser asignada al activo y se lo realiza sumando la Diferencia de importancia (***Dif de imp***) con la Importancia actual tomando en cuenta el signo en el momento de la operación.

$$importancia\_ideal = importancia\_actual + dif\_imp$$

Aplicado al activo *Datos de Usuario* la importancia ideal del activo es:

$$importancia\_ideal = 1 + (-0.01) = 0.99$$

Luego de determinar la importancia ideal debemos hacer una comparación con la importancia actual y verificar si la importancia asignada a los activos es correcta de acuerdo al nivel de riesgos al que está expuesto.

Aplicación de la Tabla 2.5: (Análisis de Importancias)

Activos	Nivel de vulnerabilidad	%	Importancia (actual)	%	Dif. de %	Dif. De Imp.	Importancia (ideal)
1 Datos de usuarios	133,33	1,1363	1	1,25	-0,11	-0,01	0,99
2 Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	257,14	2,1914	2	2,50	-0,31	-0,06	1,94
3 Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	385,71	3,2872	3	3,75	-0,46	-0,14	2,86
4 Cableado, antenas, switches, hubs, modems, routers, firewalls	700	5,9656	6	7,50	-1,53	-0,92	5,08
5 Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	688,89	5,871	4	5,00	0,87	0,35	4,35
6 Usuarios	850	7,244	5	6,25	0,99	0,50	5,50
7 Red	811,76	6,9181	6	7,50	-0,58	-0,35	5,65
8 Datos en transito, datos de configuración, datos en medios externos	1013,33	8,6359	8	10,00	-1,36	-1,09	6,91
9 Backup (respaldos de hardware, software y datos)	1350	11,505	9	11,25	0,26	0,23	9,23
10 Bases de datos	1409,09	12,009	10	12,50	-0,49	-0,49	9,51
11 Servidores	1384,62	11,8	10	12,50	-0,70	-0,70	9,30
12 Software de aplicación, programas fuente, sistemas operativos	1450	12,357	9	11,25	1,11	1,00	10,00
13 Administradores (Centros Tecnológicos)	1300	11,079	7	8,75	2,33	1,63	8,63
	11733,87	**100**	**80**	**100,00**	**0,00**	**-0,06**	**79,94**

2.1.4.7.- Valores máximos y mínimos reales

La obtención de los valores máximos y mínimos reales de riesgo nos permite determinar el porcentaje de riesgos que la Institución debe minimizar para estar dentro de los parámetros normales de riesgo de acuerdo a los factores que incurren sus activos.

En la tabla siguiente se maneja el concepto de llevar los riesgos a valores máximos y mínimos, es decir, para la aplicación actual se especificará que todos los factores tienen una probabilidad de ocurrencia de 3 como valores máximos (**333**) y probabilidad de ocurrencia de 1 como valores mínimos (**111**) sin la intervención de la importancia. Ver Aplicación de la tabla 2.3 (Cálculo de niveles de probabilidad). Y en los valores actuales (**123**) serás iguales a los obtenidos en Aplicación de la tabla 2.4 (Niveles de Vulnerabilidad) en el nivel de vulnerabilidad escala 1-1 (**imp 1-1**) mantiene la probabilidad de ocurrencia obtenida anteriormente.

Para el cálculo respectivo de los valores máximos se debe especificar las probabilidades de ocurrencia en el valor de tres y volver a recalcular la probabilidad de riesgos que el activo tiene de acuerdo a los factores de riesgos inherentes. Ver Aplicación de la tabla 2.3 (Cálculo de niveles de probabilidad) y así obtener el valor del nivel de vulnerabilidad de cada factor de riesgo que realizado en cada activo se obtuvo el valor de 300.

Aplicado al activo *Red* el valor de riesgos totales llevados al máximo valor (333) es:

$$\%\,prob.riesgos = \frac{probabilidad\_de\_ocurrencia \times 100}{cantidad\_de\_factores\_de\_riesgos}$$

$$\%\,prob.riesgos = \frac{3 \times 100}{17} = 17.64$$

Y el nivel de vulnerabilidad total del activo llevado a valores máximos es:

$$Valor\_maximo\_(333) = (\%prob.riesgos \times cantidad\_de\_factores\_de\_riesgo)$$

$$Valor\_maximo\_(333) = (17.64 \times 17) = 300$$

De igual manera, se realiza el mismo procedimiento pero cambiando la probabilidad de ocurrencia a 1 y con ello se de terminaría el porcentaje de cada activo respecto al valor máximo total, mínimo total y actual total de riesgos.

Aplicación de la Tabla 2.6: (Valores máximos y mínimos reales)

Activos - Riesgos totales (Sin ponderar la importancia)	Valores Máximos		Valores Mínimos		Valores Actuales	
	(333)	%	(111)	%	(123)	%
1 Datos de usuarios	300	7,69	100	7,69	133,33	7,06
2 Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	300	7,69	100	7,69	128,57	6,81
3 Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	300	7,69	100	7,69	128,57	6,81
4 Cableado, antenas, switches, hubs, modems, routers, firewalls	300	7,69	100	7,69	116,67	6,18
5 Documentación de programas, hardware, sistemas, procedimientos	300	7,69	100	7,69	172,22	9,12
6 Usuarios	300	7,69	100	7,69	170,00	9,01
7 Red	300	7,69	100	7,69	135,29	7,17
8 Datos en transito, datos de configuración, datos en medios externos	300	7,69	100	7,69	126,67	6,71
9 Backup (respaldos de hardware, software y datos)	300	7,69	100	7,69	150,00	7,95
10 Bases de datos	300	7,69	100	7,69	140,91	7,47
11 Servidores	300	7,69	100	7,69	138,46	7,34
12 Software de aplicación, programas fuente, sistemas operativos	300	7,69	100	7,69	161,11	8,54
13 Administradores (Centros Tecnológicos)	300	7,69	100	7,69	185,71	9,84
	3900	**100,00**	**1300**	**100,00**	**1887,52**	**100,00**

Como consecuencia del análisis anterior, se puede calcular que el porcentaje de riesgos descubiertos en la Institución es del 48,4% (1887,52 puntos), considerando el nivel máximo de riesgos como el 100% (3900 puntos), y sabiendo que el porcentaje mínimo es de 33.3% (1300 puntos).

Para el cálculo del porcentaje de riesgos descubiertos se utiliza la siguiente fórmula:

$$Porcentaje\_riesgos\_descubiertos = \frac{valor\_actual\_total(123) * 100}{valor\_maximo\_total(333)}$$

$$Porcentaje\_riesgos\_descubiertos = \frac{1887,52 * 100}{3900} = 48.40$$

Para el cálculo del porcentaje de riesgos mínimos se utiliza la siguiente fórmula:

$$Porcentaje\_riesgos\_mínimos = \frac{valor\_minimo\_total(111) * 100}{valor\_maximo\_total(333)}$$

$$Porcentaje\_riesgos\_mínimos = \frac{1300 * 100}{3900} = 33.33$$

Para el cálculo del porcentaje de riesgos a minimizar se utiliza la siguiente fórmula:

$$Porcentaje\_riesgos\_minimizar = Porcentaje\_riesgos\_descubiertos - Porcentaje\_riesgos\_mínimos$$

$$Porcentaje\_riesgos\_minimizar = 48,40 - 33,33 = 15,06$$

Por esta razón podemos concluir que la Institución debería reducir en 15.06% el porcentaje de riesgos descubiertos, para así conseguir el nivel mínimo de riesgos posible.

Aplicación de la Tabla 2.7: (Porcentajes de riesgos cubiertos)

Riesgos descubiertos:	48,40
Riesgos mínimos:	33,33
Riesgos a minimizar:	**15,06**

Figura 3.1: (Porcentaje de posibles riesgos vs. Porcentaje de riesgos descubiertos)

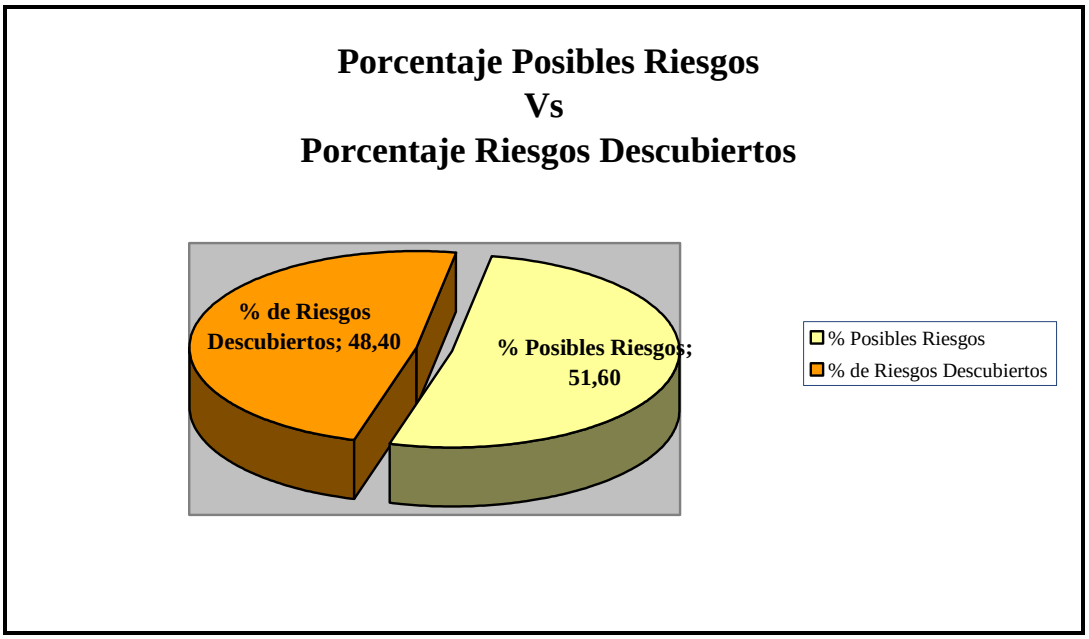
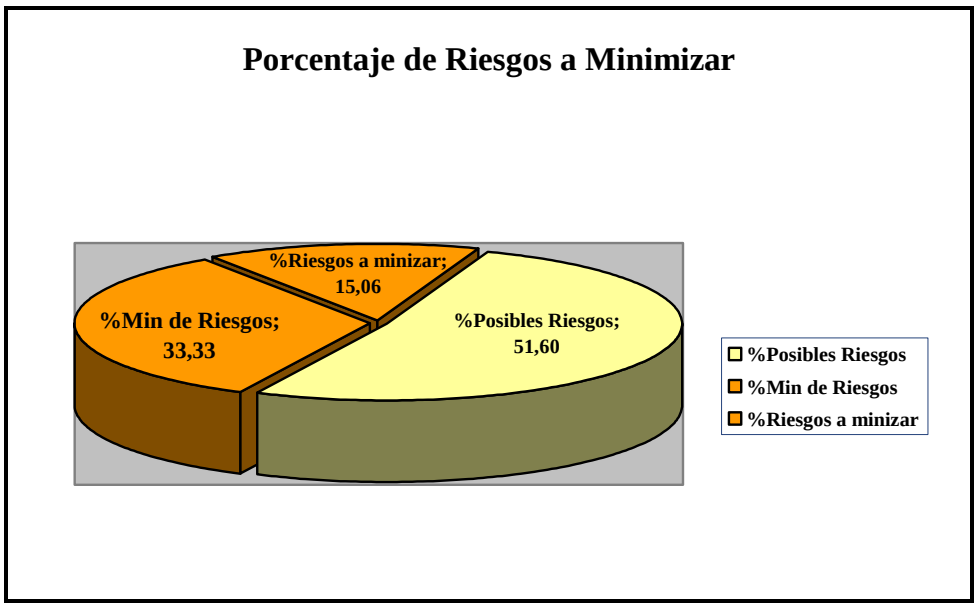


Figura 3.2: (Porcentaje de riesgos a minimizar)



Una vez realizado un análisis general de los activos de la Institución se ha creído conveniente identificar los riesgos más relevantes de cada uno de los servidores y aplicaciones principales por estar ponderados entre los activos más importantes. La probabilidad de ocurrencia tanto de las amenazas como de las vulnerabilidades esta ponderada en una Escala (1-3), siendo 1 - Bajo, 2 - Medio y 3 - Alto. La Estimación de Riesgos de cada servidor y aplicación se calculará multiplicando la probabilidad de ocurrencia de la amenaza con la probabilidad de ocurrencia de las vulnerabilidades que pueden acaecer para aquella amenaza.

Tabla 3.4: (Amenazas vs. Vulnerabilidades de los Servidores)

Nombre del Activo	Amenazas	Probabilidad Ocurrencia	Vulnerabilidades	Probabilidad Ocurrencia	Estimación Riesgo	Estimación Riesgo %
Servidor Dominio	Acceso no autorizado (borrado,modificación,etc)	2	Ubicación del servidor no seguro	2	4	8
			Falta de control de acceso	2	4	8
			Configuración de servidor no secreta	3	6	12
	Corte de luz, UPS descargado o variaciones de voltaje.	3	Capacidad insuficiente de baterías del UPS para el soporte del servicio	2	6	12
			Falla del sistema elétrico externo	1	3	6
			Análisis y mantenimiento no periódico del UPS	3	9	18
	Falla LAN, WAN	3	Falla en el cableado físico	2	6	12
			Falla en los dispositivos de red (router,switch)	1	3	6
			Mala configuración de los dispositivos	3	9	18
					50	**100**

Nombre del Activo	Amenazas	Probabilidad Ocurrencia	Vulnerabilidades	Probabilidad Ocurrencia	Estimación Riesgo	Estimación Riesgo %
Servidor Base de Datos	Acceso no autorizado (borrado,modificación,etc)	2	Ubicación del servidor no seguro	2	4	8,00
			Falta de control de acceso	2	4	8,00
			Configuración de servidor no secreta	3	6	12,00
	Corte de luz, UPS descargado o variaciones de voltaje.	3	Capacidad insuficiente de baterías del UPS para el soporte del servicio	2	6	12,00
			Falla del sistema elétrico externo	1	3	6,00
			Análisis y mantenimiento no periódico del UPS	3	9	18,00
	Robo de Información	3	Falta de confidencialidad en los datos privados	2	6	12,00
			Modificación e intercepción de datos en transito	1	3	6,00
			Mala administración de control de acceso	3	9	18,00
					50	**100**

Nombre del Activo	Amenazas	Probabilidad Ocurrencia	Vulnerabilidades	Probabilidad Ocurrencia	Estimación Riesgo	Estimación Riesgo %
Servidor Aplicaciones	No disponibilidad de las aplicaciones	3	Corte de luz	2	6	11,32
			falla LAN, WAN	2	6	11,32
			Falla servidor de dominio	3	9	16,98
	Virus	3	Falta de antivirus	2	6	11,32
			Falta de actualización de la definiciones de virus	1	3	5,66
			Falta de control de acceso al Internet	3	9	16,98
	Acceso no autorizado	2	Ubicación del servidor no seguro	2	4	7,55
			Falta de control de acceso	2	4	7,55
			Configuración de servidor no secreta	3	6	11,32
					53	**100**

Nombre del Activo	Amenazas	Probabilidad Ocurrencia	Vulnerabilidades	Probabilidad Ocurrencia	Estimación Riesgo	Estimación Riesgo %
Servidor Proxy	Spoofing y sniffing	1	Puertos de red no controlados	3	3	7,69
			Falla en el control acceso lógico	2	2	5,13
			Falta confidencialidad de las datos privados y de sistemas	2	2	5,13
	Virus	3	Falta de antivirus	2	6	15,38
			Falta de actualización de la definiciones de virus	1	3	7,69
			Falta de control de acceso al Internet	3	9	23,08
	Acceso no autorizado	2	Ubicación del servidor no seguro	2	4	10,26
			Falta de control de acceso	2	4	10,26
			Configuración de servidor no secreta	3	6	15,38
					39	**100**

Nombre del Activo	Amenazas	Probabilidad Ocurrencia	Vulnerabilidades	Probabilidad Ocurrencia	Estimación Riesgo	Estimación Riesgo %
Servidor Mail	No disponibilidad e servicio de correo	1	Corte de Luz	1	1	2,94
			Falta de servidor de dominio	1	1	2,94
			Mala configuración de correo	2	2	5,88
	Virus	3	Falta de antivirus	2	6	17,65
			Fal ta de actualizaciones de definiciones de antivirus	1	3	8,82
			Falta de control de acceso al Internet	3	9	26,47
	Falla LAN, WAN	2	Falla en el cableado físico	2	4	11,76
			Falla en los dispositivos de red (router,switch)	1	2	5,88
			Mala configuración de los dispositivos	3	6	17,65
					34	**100**

Después del análisis respectivo se obtuvo que el servidor de aplicaciones es el activo con mayor nivel de riesgo el cual debe tener mayores controles. Los servidores de Mail y Proxy fueron los de menor nivel riesgo ubicándoles como activos residuales para posteriores análisis.

Tabla 3.5: (Amenazas vs. Vulnerabilidades de las Aplicaciones)

Es de destacar que las aplicaciones presentadas fueron recopiladas de acuerdo a conversaciones mantenidas con el Director de la DIRDAI así como también los responsables directos de las aplicaciones de la Armada siendo estos quienes especificaron la importancia de las mismas y su nivel de impacto en la Institución en el caso de una amenaza.

Aplicación	Amenazas - Probabilidad Ocurrencia				Vulnerabilidades - Probabilidad Ocurrencia										
	Acceso no autorizado	Robo de información	Recursos informáticos insuficientes	Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	Acceso no autorizado		Robo de información			Recursos informáticos insuficientes			Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema		
					Falta de control de acceso lógico	Divulgación de contraseñas	Suplantación de usuarios autorizados	Impresión de documetnación	Falta de control en los servidores de aplicación y base de datos	Características de los equipos computacionales no adecuadas	Ausencia de planificación en los equipos computacionales necesarios	Falta de asignación de presupuesto para la adquisición de equipos	Falta de capacitación de los usuarios	Falta de cultura organizacional en cuanto a Seguridad Informática	Falta de control de monitoreo en la utilización de las aplicaciones
Sistema Integrado Financiero (SIF)	2	2	2	3	2	2	1	3	2	2	2	1	2	3	3
Gestión Documental	2	1	1	2	1	2	1	3	1	1	1	1	2	3	2
CANOPUS	2	2	2	2	1	2	2	3	1	1	1	1	2	3	2
Portal Web del SIF	3	2	3	3	3	1	1	2	2	3	2	2	1	3	3
Mensajería Instantanea Corporativa	1	1	2	3	2	2	2	1	2	2	1	1	1	3	2
Video Conferencia	2	1	3	1	1	1	1	1	2	3	3	3	2	3	2
Red Naval de Datos	2	2	2	3	2	1	2	2	2	2	2	1	2	3	3
Sistema Integrado de Personal (SIP)	2	2	2	3	2	2	1	3	2	2	2	1	2	3	3

Tabla 3.5: (Amenazas vs. Vulnerabilidades de las Aplicaciones) Segunda Parte

Aplicación	Estimación de Riesgo											Total de Estimación de Riesgo	Estimación de Riesgo %											Total de Estimación de Riesgo %
	Falta de control de acceso lógico	Divulgación de contraseñas	Suplantación de usuarios autorizados	Impresión de documetnación	Falta de control en los servidores de aplicación y base de datos	Características de los equipos computacionales no adecuadas	Ausencia de planificación en los equipos computacionales necesarios	Falta de asignación de presupuesto para la adquisición de equipos	Falta de capacitación de los usuarios	Falta de cultura organizacional en cuanto a Seguridad Informática	Falta de control de monitoreo en la utilización de las aplicaciones		Falta de control de acceso lógico	Divulgación de contraseñas	Suplantación de usuarios autorizados	Impresión de documetnación	Falta de control en los servidores de aplicación y base de datos	Características de los equipos computacionales no adecuadas	Ausencia de planificación en los equipos computacionales necesarios	Falta de asignación de presupuesto para la adquisición de equipos	Falta de capacitación de los usuarios	Falta de cultura organizacional en cuanto a Seguridad Informática	Falta de control de monitoreo en la utilización de las aplicaciones	
Sistema Integrado Financiero (SIF)	4	4	2	6	4	4	4	2	6	9	9	54	7,407	7,407	3,704	11,11	7,407	7,407	7,407	3,704	11,11	16,67	16,67	100
Gestión Documental	2	4	1	3	1	1	1	1	4	6	4	28	7,143	14,29	3,571	10,71	3,571	3,571	3,571	3,571	14,29	21,43	14,29	100
CANOPUS	2	4	4	6	2	2	2	2	4	6	4	38	5,263	10,53	10,53	15,79	5,263	5,263	5,263	5,263	10,53	15,79	10,53	100
Portal Web del SIF	9	3	2	4	4	9	6	6	3	9	9	64	14,06	4,688	3,125	6,25	6,25	14,06	9,375	9,375	4,688	14,06	14,06	100
Mensajería Instantanea Corporativa	2	2	2	1	2	4	2	2	3	9	6	35	5,714	5,714	5,714	2,857	5,714	11,43	5,714	5,714	8,571	25,71	17,14	100
Video Conferencia	2	2	1	1	2	9	9	9	2	3	2	42	4,762	4,762	2,381	2,381	4,762	21,43	21,43	21,43	4,762	7,143	4,762	100
Red Naval de Datos	4	2	4	4	4	4	4	2	6	9	9	52	7,692	3,846	7,692	7,692	7,692	7,692	7,692	3,846	11,54	17,31	17,31	100
Sistema Integrado de Personal (SIP)	4	4	2	6	4	4	4	2	6	9	9	54	7,407	7,407	3,704	11,11	7,407	7,407	7,407	3,704	11,11	16,67	16,67	100

Después del análisis respectivo se obtuvo que las aplicaciones: Portal Web del SIF, SIF y SIP son los activos con mayor nivel de riesgo el cual debe tener mayores controles. Las aplicaciones: Gestión Documental, CANOPUS y Mensajería Instantánea fueron los de menor nivel riesgo ubicándoles como activos residuales para posteriores análisis.

Capítulo 4. Arquitectura de la Seguridad Informática

4.1.- Identificación de las Áreas, Políticas y Estándares de Seguridad

En base al análisis de riesgos elaborado anteriormente y con la documentación de la Norma ISO 17799 Tecnología de Información – Código de Práctica para la Gestión de la Seguridad de la Información, se realizó la elaboración de las Políticas y Estándares de Seguridad para la Armada del Ecuador.

4.1.1.- Área Lógica

4.1.1.1.- Políticas y Estándares de Seguridad

La realización de las Políticas y Estándares de Seguridad se lo realizó mediante los controles descritos en la Norma ISO 17799, seleccionando solo los controles que son aplicables para la Armada del Ecuador. Así mismo, existen otras políticas que se desarrollaron en base el análisis del Plan Estratégico de las Tecnologías de Información de la Institución *(PETI)* y de su situación actual obtenida de las encuestas y el análisis de riesgos respectivo, por tal motivo se especificará de donde se obtuvo cada política, al final de las mismas.

Políticas para el Control de Acceso del Usuario

Registro de usuarios

Elaborar un procedimiento formal de registro de usuarios para otorgar acceso a los sistemas y servicios de información.

- Estandarizar en los Centros Tecnológicos de Información los parámetros almacenados en los perfiles de Usuarios. *(Análisis de la Situación actual)*
- Requerir a los usuarios que firmen declaraciones indicando que entienden las condiciones de acceso al sistema. *(Norma ISO 17799 - 9.2.1 Registro del Usuario)*

- Eliminar inmediatamente los derechos de acceso de los usuarios que hayan cambiado de trabajo o hayan dejado la Institución. *(Norma ISO 17799 - 9.2.1 Registro del Usuario)*
- Chequear de manera periódica, y eliminar los IDs de cuentas de usuario redundantes. *(Norma ISO 17799 - 9.2.1 Registro del Usuario)*
- Asegurar que no se emitan IDs de usuario redundantes a otros usuarios. *(Norma ISO 17799 - 9.2.1 Registro del Usuario)*
- Cuando el usuario deje de tener relación oficial con la Institución o la cuenta deje de ser utilizada por un tiempo definido más de 30 días, la cuenta deberá ser removida, para lo cual los jefes de personal de cada reparto deben notificar a los Centros Tecnológicos (Quito-Guayaquil) para el procedimiento respectivo. (*PETI)*
- Cuando el usuario deje de laborar o de tener una relación con la Institución, el departamento de sistemas deberá ser notificado con un memorando u oficio a fin de que los administradores de sistemas procedan a tomar las medidas pertinentes con su información y cuenta de acceso. (*PETI)*
- Los usuarios predeterminados por los sistemas operativos deben ser eliminados por el Administrador de Redes. *(Análisis de la Situación Actual)*

Permisos de usuarios

Restringir y controlar la asignación y uso de los privilegios a los usuarios, el uso inapropiado de los privilegios del sistema con frecuencia es un importante factor que contribuye a la falla de los sistemas que se han violado.

- El Administrador de Redes en el único encargado de la asignación de permisos a los usuarios. *(Análisis de la Situación Actual)*

- Identificar los privilegios asociados con el sistema, así como la asignación de los privilegios a las personas sobre una base "lo que necesitan saber" y "evento por evento"; es decir, el requerimiento mínimo para su rol funcional sólo cuando se necesita. *(Norma ISO 17799 - 9.2.2 Manejo de Privilegios)*
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se debieran otorgar sino hasta que se complete el proceso de autorización. *(Norma ISO 17799 - 9.2.2 Manejo de Privilegios)*

Mantenimiento y Revisión de privilegios

Mantener un control efectivo sobre el acceso a los datos y servicios de información. Los Centros Tecnológicos deben realizar un proceso formal en intervalos regulares para revisar los derechos de acceso de los usuarios.

- Revisar los derechos de acceso de los usuarios a intervalos regulares (se recomienda un periodo de 6 meses). *(Norma ISO 17799 - 9.2.4 Revisión de los derechos de acceso del usuario)*
- Revisar las autorizaciones para derechos de acceso privilegiados a intervalos más frecuentes (se recomienda un periodo de 3 meses). *(Norma ISO 17799 - 9.2.4 Revisión de los derechos de acceso del usuario)*
- Chequear las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados. *(Norma ISO 17799 - 9.2.4 Revisión de los derechos de acceso del usuario)*

Manejo de contraseñas del usuario

Las claves secretas son medios comunes para validar la identidad del usuario para tener acceso al sistema o servicio de información. La asignación de contraseñas secretas se debiera controlar a través de un proceso de gestión formal.

- Requerir a los usuarios que firmen una declaración para mantener confidenciales sus claves secretas personales y las contraseñas secretas del trabajo en grupo solamente dentro del grupo. *(Norma ISO 17799 - 9.2.3 Manejo de la clave secreta del usuario)*

- Asegurar cuando se requiera a los usuarios que mantengan sus propias contraseñas secretas, que se les proporcione inicialmente una contraseña secreta temporal que están obligados a cambiar inmediatamente. Las contraseñas secretas temporales provistas cuando los usuarios olvidan su contraseña secreta sólo se debieran suministrar después de una identificación positiva del usuario. *(Norma ISO 17799 - 9.2.3 Manejo de la clave secreta del usuario)*
- Evitar que las contraseñas se guarden en el sistema de cómputo en una forma desprotegida. *(Norma ISO 17799 - 9.2.3 Manejo de la clave secreta del usuario)*
- El acceso y custodia de todas las contraseñas de los usuarios es absoluta responsabilidad del Administrador de la Red siendo este el único responsable de su confidencialidad hasta la entrega al usuario final. *(PETI)*

Uso de contraseñas por parte de los usuarios

La cooperación de los usuarios autorizados es esencial para una seguridad, los usuarios debieran estar concientes de sus responsabilidades para mantener controles de acceso efectivos particularmente con relación al uso de contraseñas secretas y la seguridad del equipo.

- Mantener sus contraseñas secretas en forma confidencial. *(Norma ISO 17799 - 9.3.1 Uso de clave secreta)*
- Evitar mantener un registro escrito de sus contraseñas secretas, a no ser que se puedan guardar con seguridad. *(Norma ISO 17799 - 9.3.1 Uso de clave secreta)*

- Cambiar su contraseña secreta cuando exista algún indicio de una posible violación en el sistema o contraseña secreta. *(Norma ISO 17799 - 9.3.1 Uso de clave secreta)*
- Seleccionar contraseñas con un largo mínimo de seis a ocho caracteres que sean fáciles de recordar. *(Norma ISO 17799 - 9.3.1 Uso de clave secreta)*
- Elaborar las contraseñas no basándose en algo que otra persona pueda adivinar fácilmente o que se puede obtener utilizando información relacionada con la persona, como nombres, número de teléfono, fechas de nacimiento, etc. *(Norma ISO 17799 - 9.3.1 Uso de clave secreta)*
- Evitar que las contraseñas contengan caracteres idénticos consecutivos o grupos de sólo números o letras. *(Norma ISO 17799 - 9.3.1 Uso de clave secreta)*
- Cambiar la contraseña por lo menos una vez cada 30 días usando las políticas de creación de contraseña. *(Análisis de la Situación Actual)*

Sugerencia: Si los usuarios necesitan tener acceso a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se les debiera advertir que pueden utilizar una sola contraseña.

Equipos de usuario desatendido

Los usuarios debieran asegurarse que el equipo desatendido tenga la protección apropiada. El equipo instalado en áreas de usuarios como estaciones de trabajo o servidores de archivo, puede requerir protección específica del acceso no autorizado cuando se deja desatendido por un periodo extenso.

- Finalizar las sesiones activas cuando terminen, a no ser que puedan asegurarse mediante mecanismos de bloqueo apropiados como una pantalla asegurada mediante una clave secreta. *(Norma ISO 17799 - 9.3.2 Equipo de usuario desatendido)*

- Apagar las computadoras cuando acaban su trabajo. *(Norma ISO 17799 - 9.3.2 Equipo de usuario desatendido)*
- Asegurar las PCs o terminales del uso no autorizado mediante una tecla de bloqueo o un control equivalente (acceso con clave secreta). *(Norma ISO 17799 - 9.3.2 Equipo de usuario desatendido)*

Políticas para el Control de Acceso al Sistema Operativo

Identificación y autenticación del usuario

Todos los usuarios (incluyendo el personal de soporte técnico, como operadores, administradores de redes, programadores de sistemas y administradores de bases de datos) debieran tener un identificador único (ID del usuario) para su uso personal y singular de manera que las actividades pueden ser subsecuentemente monitoreadas a las personas responsables. *(Norma ISO 17799 - 9.5.3 Identificación y autenticación del usuario)*

- Los IDs de ingreso a la red, los sistemas y los recursos informáticos tanto físicos como lógicos son propiedad de la Institución y se usarán exclusivamente para actividades relacionadas con ella. *(PETI)*
- Ninguna ID de usuario podrá ser usada para propósitos ilegales, criminales o no éticos. *(PETI)*

Inicio de sesión en un terminal

El acceso a los servicios de información se debiera obtener vía un proceso de inicio de sesión seguro.

- No presentar los identificadores del sistema o la aplicación hasta que se haya completado exitosamente el proceso de inicio de sesión. *(Norma ISO 17799 - 9.5.2 Procedimientos para el inicio de sesión (log in) en un Terminal)*

- Presentar una advertencia general que a esa computadora sólo tienen acceso los usuarios autorizados. *(Norma ISO 17799 - 9.5.2 Procedimientos para el inicio de sesión (log in) en un Terminal)*
- Evitar la presentación de mensajes de asistencia que ayuden a un usuario no autorizado durante el procedimiento de inicio. *(Norma ISO 17799 - 9.5.2 Procedimientos para el inicio de sesión (log in) en un Terminal)*
- Validar la información de inicio de sesión sólo después de haber llenado todos los datos. Si surge un error el sistema no debiera indicar qué datos son correctos o incorrectos. *(Norma ISO 17799 - 9.5.2 Procedimientos para el inicio de sesión (log in) en un Terminal)*
- Limitar el número de intentos de inicios de sesión fallidos permitidos (tres intentos es lo recomendado). *(Norma ISO 17799 - 9.5.2 Procedimientos para el inicio de sesión (log in) en un Terminal)*
    - registrar los intentos fallidos.
    - establecer un tiempo de espera antes de permitir más intentos de inicio o rechazar cualquier otro intento sin una autorización específica.
    - desconectar las conexiones de enlace.
- Presentar la siguiente información al completar un inicio de sesión exitoso: *(Norma ISO 17799 - 9.5.2 Procedimientos para el inicio de sesión (log in) en un Terminal)*
    - fecha y hora del inicio exitoso anterior;
    - detalles de cualquier intento de inicio fallido desde el último inicio exitoso.

Terminales Inactivas

Las terminales inactivas debieran cerrarse después de un periodo definido de inactividad para evitar el acceso de personas no autorizadas, este medio de cierre debiera

limpiar la pantalla del terminal y cerrar tanto las aplicaciones como las sesiones en red. *(Norma ISO 17799 - 9.5.7 Terminales inactivas)*

Monitoreo del acceso del sistema

Producir y mantener registros de auditoria que detallen las excepciones y otros eventos relevantes a la seguridad para un periodo acordado para ayudar al monitoreo del acceso del sistema, incluyendo: *(Norma ISO 17799 - 9.7.1 Registro de eventos)*

- ID`s de los de usuario
- Fechas y horas de ingresos y salidas
- Identidad del terminal o locación si fuese posible
- Registros de intentos exitosos y rechazados de acceso al sistema
- Registros de intentos exitosos y rechazados de acceso a datos y otros recursos

Monitoreo del uso del sistema

Se deban establecer procedimientos para el monitoreo del uso de medios de procesamiento de información, asegurando que los usuarios sólo realicen actividades para las cuales han sido autorizados. *(Norma ISO 17799 - 9.7.2 Monitoreo del uso del sistema)*

a. acceso autorizado, incluyendo:
    a. ID del usuario:
    b. fecha y hora de eventos claves (tipos de eventos)
    c. archivos a los cuales se tuvo acceso
    d. el programa/utilidades utilizados
b. intentos de accesos no autorizados, como:
    a. intentos fallidos

b. violaciones de la política de acceso y los avisos para los portales y firewalls de la red
c. alertas de los sistemas de detección de intrusión propios

c. alertas o fallas en el sistema, como:
   a. alertas o mensajes en la consola
   b. excepciones en el registro del sistema
   c. alarmas en el manejo de la red

El resultado de las actividades de monitoreo se debiera revisar regularmente, la frecuencia de la revisión dependerá de los riesgos involucrados. Se deberían incluir:

- el grado crítico de los procesos de aplicación
- el valor, sensibilidad y grado critico de la información involucrada
- la experiencia previa de infiltración y mal uso del sistema
- el grado de interconexión del sistema (particularmente con redes públicas).

Políticas de Control de Acceso a la Aplicación

Restricción al acceso a la información

Los usuarios de los sistemas de aplicación, incluyendo el personal de apoyo, debieran tener un acceso a las funciones de los sistemas de información y aplicación en concordancia con una política de control de acceso definida, basado en los requerimientos de la política de acceso a la información Institucional.

- Restringir el conocimiento de los usuarios sobre las funciones del sistema de información o aplicación para las cuales no tienen acceso autorizado con la edición apropiada de la documentación del usuario. *(Norma ISO 17799 - 9.6.1 Restricción al acceso a la información)*

- Controlar los derechos de acceso de los usuarios (leer, escribir, eliminar y ejecutar). *(Norma ISO 17799 - 9.6.1 Restricción al acceso a la información)*
- Asegurar que los datos de salida de los sistemas de aplicación que manejan información confidencial sólo contengan información relevante y sólo se envíe a terminales y locaciones autorizadas. *(Norma ISO 17799 - 9.6.1 Restricción al acceso a la información)*

Sistema sensible o confidencial

Los sistemas sensibles o confidenciales deben requerir un ambiente de cómputo dedicado. Algunos sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial y requieren de un trato especial.

- Identificar la sensibilidad de un sistema de aplicación explícitamente por el propietario de la aplicación. *(Norma ISO 17799 - 9.6.2 Aislamiento del sistema sensible o confidencial)*

<u>Políticas para el manejo de la Información</u>

Educación y capacitación en seguridad de la información

Todos los empleados de la Institución y, cuando sea relevante, las terceras personas debieran recibir una capacitación apropiada y actualizaciones regulares sobre las políticas y procedimientos Institucionales. Esto incluye los requerimientos de seguridad, responsabilidades legales y controles, así como el uso correcto de los medios de procesamiento de la información, antes de concederles acceso a la información o servicios. *(Norma ISO 17799 - 6.2.1 Educación y capacitación en seguridad de la información)*

- Prohibir el almacenamiento de información clasificada como secretísima y secreta en las estaciones de trabajo, la misma que debe ser manejada de acuerdo al manual de administración de documentación de la Institución. *(PETI)*

- Los usuarios deberán utilizar únicamente los servicios para los cuales están autorizadas. Los usuarios no pueden utilizar las cuentas de otras personas ni intentar de apoderarse de las claves de acceso, como tampoco intentar burlar los sistemas de seguridad bajo ningún punto de vista. *(PETI)*
- Cada usuario de un Pc será responsable de mantener los debidos resguardos en cuanto a confidencialidad de los datos almacenados. *(PETI)*

Medios de información y de procesamiento de información

La información y los medios de información debieran ser protegidos de una divulgación, modificación o robo por personas no autorizados, y se debieran establecer controles para minimizar la pérdida o daño.

- Almacenar adecuadamente en archivadores y/o otras formas de muebles seguros los medios en documentos y computadora cuando no están en uso, especialmente fuera de las horas de trabajo. *(Norma ISO 17799 - 7.3.1 Política de escritorio vacío y pantalla vacía)*
- Guardar la información confidencial o crítica en una caja fuerte o archivadora resistente al fuego cuando no se la requiera. *(Norma ISO 17799 - 7.3.1 Política de escritorio vacío y pantalla vacía)*
- Proteger los puntos de ingreso y salida de correo y las máquinas de fax desatendidos. *(Norma ISO 17799 - 7.3.1 Política de escritorio vacío y pantalla vacía)*
- Las fotocopiadoras debieran mantenerse aseguradas fuera de las horas de trabajo normales. *(Norma ISO 17799 - 7.3.1 Política de escritorio vacío y pantalla vacía)*

- La información confidencial o clasificada, cuando está impresa, debiera ser eliminada de las impresoras inmediatamente. *(Norma ISO 17799 - 7.3.1 Política de escritorio vacío y pantalla vacía)*

Backup de la Información

Generar copias de backup de la información y software esencial de manera regular.

- Mantener en un local remoto un nivel mínimo de información backup, junto con registros exactos y completos de las copias backup y los procedimientos de restauración documentados, a una distancia suficiente para escapar a cualquier daño de un desastre en el departamento. *(Norma ISO 17799 - 8.4.1 Backup de la Información)*
- Probar regularmente los medios de backup para asegurar que se pueda confiar en ellos para un uso de emergencia cuando sea necesario. *(Norma ISO 17799 - 8.4.1 Backup de la Información)*
- Los respaldos serán de dos tipos, diario y semanal. *(PETI)*
- El respaldo diario se lo realizará al cierre de las operaciones. *(PETI)*
- El respaldo semanal se realizará el día viernes al cierre de las operaciones. *(PETI)*
- El respaldo debe ser realizado por el personal responsable del mismo. *(PETI)*

Mantenimiento de registro de actividades

El personal operacional debe mantener un registro de sus actividades en el sistema y registrar las fallas reportadas por los usuarios de los sistemas de procesamiento de la información y comunicaciones. Los registros deben incluir: *(Norma ISO 17799 - 8.4.2 Registros del operador)*

- momento de Inicio y fin de los sistemas.
- errores del sistema y las acciones correctivas tomadas.

- confirmación del manejo correcto de los archivos de datos y salidas de computación.
- el nombre de la persona que está realizando el ingreso en el registro.

Para el manejo de fallas deben incluir: *(Norma ISO 17799 - 8.4.3 Registro de fallas)*

- revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente.
- revisión de las medidas correctivas para asegurar que los controles no se hayan comprometido y que la acción tomada esté completamente autorizada.

Documentación del sistema

La documentación del sistema puede contener un rango de información importante (descripciones de los procesos de aplicación, procedimientos, estructuras de datos, procesos de autorización).

- Almacenar de manera segura la documentación del sistema. *(Norma ISO 17799 - 8.6.4 Seguridad de la documentación del sistema)*
- Proteger apropiadamente la documentación del sistema que se mantiene en una red pública. *(Norma ISO 17799 - 8.6.4 Seguridad de la documentación del sistema)*

4.1.2.- Área Física

4.1.2.1.- Políticas y Estándares de Seguridad

Políticas de Seguridad Institucional

Reuniones de la Directiva sobre seguridad de la información

La seguridad de la información es una responsabilidad compartida por todos los miembros de la directiva, por lo tanto, se debiera considerar un foro para asegurar que exista una dirección clara y un apoyo visible para las iniciativas de seguridad.

- Establecer los roles y responsabilidades específicos para la seguridad de la información en toda la organización. *(Norma ISO 17799 - 4.1.1 Foro gerencial de seguridad de la información)*
- Establecer las metodologías y procesos específicos para la seguridad de la información (evaluación de riesgo, sistema de clasificación de seguridad). *(Norma ISO 17799 - 4.1.1 Foro gerencial de seguridad de la información)*
- Establecer y respaldar las iniciativas de información a nivel de toda la organización (programa de conciencia de seguridad). *(Norma ISO 17799 - 4.1.1 Foro gerencial de seguridad de la información)*
- Evaluar la idoneidad y coordinar la implementación de los controles específicos de seguridad de la información para sistemas o servicios nuevos. *(Norma ISO 17799 - 4.1.1 Foro gerencial de seguridad de la información)*
- Revisiones de los incidentes de seguridad de la información. *(Norma ISO 17799 - 4.1.1 Foro gerencial de seguridad de la información)*
- Promover la publicidad de las políticas de la Seguridad de la Información. *(Norma ISO 17799 - 4.1.1 Foro gerencial de seguridad de la información)*
- El administrador de redes deberá realizar un informe por escrito de los empleados que infrinjan repetidamente las políticas de seguridad, siguiendo el órgano regula correspondiente, para que sean sancionados. *(PETI)*
- Se debe tener los mismos tipos de Administradores (base de datos, aplicaciones, redes y comunicaciones) en ambos Centros Tecnológicos para el manejo de los sistemas Institucionales. *(Análisis de la Situación Actual)*

- La aplicación de políticas, normas, procedimientos y uso de aplicaciones para el control de Seguridad Informática debe ser estandarizada en ambos Centros Tecnológicos. *(Análisis de la Situación Actual)*

Clasificación de la Información

Asegurar que los activos de información reciban un nivel de protección apropiado, clasificada por necesidades, prioridades y grado de protección, verificando los varios grados de sensibilidad y criticidad. *(Norma ISO 17799 - 5.2 Clasificación de la información)*

Plan de Contingencias

- Elaborar un Plan de Contingencias en el cual especifique los procedimientos a seguir en caso de un desastre (antes, durante y después del desastre), con sus respectivos responsables del cumplimiento de los procedimientos. *(Análisis de la Situación Actual)*
- Revisar, actualizar y analizar el Plan de Contingencias de manera anual o según eventualidades ocurridas en la Institución. *(Análisis de la Situación Actual)*
- Realizar procedimientos de concientización sobre la importancia del Plan de Contingencias. *(Análisis de la Situación Actual)*
- Realizar charlas informativas al personal de los procedimientos existentes en el Plan de Contingencias, así como también realizar simulacros del mismo, para así recabar información para el mejoramiento del Plan. *(Análisis de la Situación Actual)*

Políticas para manejo de equipos

Equipos Móviles

Cuando se utiliza medios de computación móvil, como notebooks, palms, laptops y teléfonos móviles, se debiera tener cuidado de asegurar que no se comprometa la información.

- Incluir los requerimientos de protección física, controles de acceso, técnicas de criptografía, backups y protección contra virus. *(Norma ISO 17799 - 9.8.1 Computación móvil)*
- Mantener actualizados los procedimientos contra el software malicioso. *(Norma ISO 17799 - 9.8.1 Computación móvil)*
- Asegurar el equipo que contiene información importante, sensible y/o crítica bajo llave o algún tipo de seguro. *(Norma ISO 17799 - 9.8.1 Computación móvil)*
- Establecer la capacitación para el personal que usa computación móvil para elevar su conocimiento sobre los riesgos adicionales resultantes. *(Norma ISO 17799 - 9.8.1 Computación móvil)*

Lista de activos

Elaborar una lista de activos de la Institución para conocer la importancia, valor, niveles de protección, y ubicación del activo. Se debe incluir como activo a:

- a los activos de información bases de datos y archivos de datos, documentación, manual del usuario, material de capacitación, procedimientos operacionales y de apoyo, planes de continuidad, acuerdos de reserva, información archivada. *(Norma ISO 17799 - 5.1.1 Inventario e activos)*
- activos de software: software de aplicación, software del sistema, herramientas y servicios de desarrollo. *(Norma ISO 17799 - 5.1.1 Inventario e activos)*

- activos físicos equipo de cómputo (procesadores, rnonitores, laptops, módems, etc.), equipo de comunicación (routers, switches, cableado, maquinas contestadotas, etc.), medios magnético (cintas y discos), otro equipo técnico (suministros de energía, unidades de aire acondicionado), muebles, ambientes. *(Norma ISO 17799 - 5.1.1 Inventario e activos)*
- servicios de computación y servicios de comunicaciones, servicios generales, como: calefacción, iluminación, energía, aire acondicionado. *(Norma ISO 17799 - 5.1.1 Inventario e activos)*

Mantenimiento de equipo

El equipo debiera ser mantenido correctamente para asegurar la disponibilidad e integridad continua.

- Mantener el equipo en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor. (*Norma ISO 17799 - 7.2.4 Mantenimiento de equipo)*
- Realizar las reparaciones y servicio al equipo con el personal de mantenimiento de hardware del Centro Tecnológico. (*Norma ISO 17799 - 7.2.4 Mantenimiento de equipo)*
- Mantener registros de todas las fallas sospechadas o reales y de todo el mantenimiento preventivo y correctivo. (*Norma ISO 17799 - 7.2.4 Mantenimiento de equipo)*
- Mantener los controles apropiados cuando se envía equipo fuera del departamento para mantenimiento. (*Norma ISO 17799 - 7.2.4 Mantenimiento de equipo)*
- Prohibir a los usuarios abrir las máquinas, hacer cambios no autorizados en el hardware, sea cambios de memorias, discos y mas partes constitutivas del equipo. *(PETI)*

- La división de mantenimiento deberá elaborar un cuadro de mantenimiento preventivo trimestral o semestral de acuerdo a la disponibilidad de tiempo y personal. *(PETI)*
- Restringir el cambio de configuración de los equipos que se ha sido determinado por el CETEIN respectivo. *(Análisis de la Situación Actual)*
- Estandarizar las configuraciones de las estaciones de trabajo administradas por ambos Centros Tecnológicos. *(Análisis de la Situación Actual)*
- Realizar un inventario de equipos con los respectivos números de serie (teclado, mouse, monitor, CPU),modelo, software instalado y responsable del equipo. Es importante que se verifique con el usuario la constancia del inventario realizado, así como la firma de las dos partes. *(Análisis de la Situación Actual)*

Ubicación y protección del equipo

El equipo debiera ser ubicado o protegido de manera que se reduzcan los riesgos de los peligros ambientales y las oportunidades para un acceso no autorizado.

- Monitorear las condiciones ambientales para detectar condiciones que podrían afectar adversamente a la operación de los medios de procesamiento de la información. *(Norma ISO 17799 - 7.2.1 Ubicación y protección del equipo)*
- Considerar el impacto de un desastre que ocurra cerca al departamento por ejemplo, un incendio en un edificio vecino, filtración de agua del techo o pisos por debajo del nivel del suelo. *(Norma ISO 17799 - 7.2.1 Ubicación y protección del equipo)*
- Ubicar los equipos de manera que se minimice el acceso innecesario a las áreas de trabajo. *(Norma ISO 17799 - 7.2.1 Ubicación y protección del equipo)*
- Prohibir comer, beber y fumar en las cercanías a los medios de procesamiento de la información. *(Norma ISO 17799 - 7.2.1 Ubicación y protección del equipo)*

Equipos y dispositivos

- Todo equipo computacional y de comunicación de datos pertenecientes a la Armada deberán permanecer en el lugar asignado por los Centros Tecnológicos, adicionalmente restringir la conexión de dispositivos a las PCs que no sean suministradas por los Centros Tecnológicos y en el caso de necesitarlo se debe solicitar la autorización respectiva. *(Análisis de la Situación Actual)*
- Estandarizar en ambos Centros Tecnológicos los servidores de Dominio, Base de datos, Aplicaciones, Proxy. Mail, Firewall, así como los sistemas operativos y aplicaciones para el desarrollo Institucional. *(Análisis de la Situación Actual)*
- Disponer de servidores de backup en caso de una emergencia para así tener el menor impacto dentro de la Institución. *(Análisis de la Situación Actual)*

Suministros de energía

El equipo debiera ser protegido de fallas de energía, y otras anomalías eléctricas, se debiera proporcionar un suministro eléctrico adecuado que satisfaga las especificaciones de la red.

- Incluir múltiples alimentadores para evitar un solo punto de falla en el suministro de energía. *(Norma ISO 17799 - 7.2.2 Suministros de energía)*
- Utilizar un suministro de energía sin interrupciones (UPS), realizando su chequeo regularmente para asegurar que tiene la capacidad adecuada. *(Análisis de la Situación Actual)*
- Utilizar un generador de reserva para que el procesamiento continúe en caso de una falla de energía prolongada. *(Análisis de la Situación Actual)*
- Aplicar la protección contra rayos (pararrayos) en todos los edificios. *(Análisis de la Situación Actual)*

Cableado

El cableado de energía y telecomunicaciones que lleva datos o sostiene los servicios de información se debieran proteger de la interceptación o daño.

- Implementar líneas de energía y telecomunicaciones subterráneas, para el ingreso a los medios de procesamiento de información. *(Norma ISO 17799 - 7.2.3 Seguridad en el cableado)*
- Proteger el cableado de la red de una interceptación no autorizada o daño, utilizando conductos porta cables o al evitar las rutas a través de áreas públicas. *(Norma ISO 17799 - 7.2.3 Seguridad en el cableado)*
- Separar los cables de energía de los cables de comunicaciones para evitar la interferencia. *(Norma ISO 17799 - 7.2.3 Seguridad en el cableado)*
- Para los sistemas sensibles o críticos los controles adicionales a considerarse incluyen: *(Norma ISO 17799 - 7.2.3 Seguridad en el cableado)*
    - la instalación de conductos porta cables blindados y habitaciones o cajas cerradas en los puntos de inspección y terminación
    - uso de rutas o medios de transmisión alternativos
    - uso de cableado de fibra óptica

Mantenimiento del Centro Cómputo

Al interior del Centro de Cómputo se deberá tener las condiciones apropiadas de, temperatura 10° a 15° C y humedad (aire acondicionado), piso antiestático y se deberá contar con protección contra incendios tanto los detectores de humo como los extintores, así como su respectivo mantenimiento periódico. (*PETI*)

Manejo de los medios computarizados removibles

Realizar procedimientos para el manejo de los medios computarizados removibles (cintas, discos, casetes y reportes impresos).

- Borrar los contenidos previos de cualquier medio re-usable que va a ser retirado de la Institución. *(Norma ISO 17799 - 8.6.1 Manejo de los medios computarizados removibles)*
- Realizar un registro de todos los medios retirados de la Institución previa su autorización. *(Norma ISO 17799 - 8.6.1 Manejo de los medios computarizados removibles)*
- Almacenar en un ambiente seguro los medios de almacenamiento. *(Norma ISO 17799 - 8.6.1 Manejo de los medios computarizados removibles)*

Eliminación de los medios

Cuando ya no se requieran los medios debieran ser eliminados de una manera segura, la información confidencial puede filtrarse a personas externas a través de una eliminación negligente de los medios.

- Almacenar y eliminar de una manera segura (incineración o trituración) los medios que contienen información sensible (cintas, disquetes, grabaciones de voz, documentación en papel). *(Norma ISO 17799 - 8.6.2 Eliminación de los medios)*

Políticas para el acceso físico

Barreras Físicas

La protección física se puede lograr creando varias barreras físicas (una pared, control mediante tarjetas o una recepcionista) alrededor del departamento y los medios de procesamiento de la información.

- Implementar mecanismos de control (alarmas, seguros) en el área que albergue los medios de procesamiento de información. *(Norma ISO 17799 - 7.1.1 Perímetro de seguridad física)*
- Establecer un área de recepción con personal u otros medios de control de acceso físico al departamento o edificio. *(Norma ISO 17799 - 7.1.1 Perímetro de seguridad física)*

Controles de ingreso físico

Se debieran proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que sólo se permita el ingreso del personal autorizado.

- Registrar fecha y hora de ingreso de los visitantes que van a las áreas seguras. *(Norma ISO 17799 - 7.1.2 Controles de ingreso físico)*
- Controlar el acceso a la información sensible y los medios de procesamiento de información sólo las personas autorizadas. Utilizando controles de autenticación, como: lectora de tarjetas para autorizar y validar todo acceso. *(Norma ISO 17799 - 7.1.2 Controles de ingreso físico)*
- Requerir que todo el personal use alguna forma de identificación visible y se debiera fomentar que cuestionen a las personas extrañas o cualquier que no esté utilizando la identificación visible. *(Norma ISO 17799 - 7.1.2 Controles de ingreso físico)*

Asegurar oficinas, salas y medios

La selección y diseño de un área segura debiera tomar en cuenta la posibilidad de daño por incendio, inundación, explosión y otras formas de desastre natural.

- Dar la mínima indicación del propósito de los departamentos, evitando signos obvios dentro o fuera que identifiquen la presencia de actividades de procesamiento de la información. *(Norma ISO 17799 - 7.1.3 Asegurar oficinas, salas y medios)*
- Situar las funciones y equipos de apoyo (fotocopiadoras, fax) dentro del área segura para evitar las demandas de acceso, que podrían comprometer la información. *(Norma ISO 17799 - 7.1.3 Asegurar oficinas, salas y medios)*
- Colocar sistemas adecuados para la detección de intrusos instalados de acuerdo a estándares profesionales y se debieran probar regularmente para cubrir todas las puertas externas y ventanas accesibles. *(Norma ISO 17799 - 7.1.3 Asegurar oficinas, salas y medios)*
- Separar los medios de procesamiento de información manejados por la Institución de terceras personas. *(Norma ISO 17799 - 7.1.3 Asegurar oficinas, salas y medios)*
- Situar el equipo de reserva y medios de backup a una distancia prudencial para evitar el daño en caso de desastre en el área de equipos. *(Norma ISO 17799 - 7.1.3 Asegurar oficinas, salas y medios)*

Contratos con terceras personas

Los acuerdos que involucran el acceso de terceras personas a los medios de procesamiento de información Institucional se debieran basar en un contrato formal conteniendo, o refiriéndose a, todos los requerimientos de seguridad para asegurar la conformidad con las políticas y estándares de seguridad de la organización. El contrato debe contener: *(Norma ISO 17799 - 4.2.2 Requerimientos de seguridad para los contratos con terceras personas)*

- La política general sobre la seguridad de la información
- Protección de activos, incluyendo

a. procedimientos para proteger los activos Institucionales, incluyendo la información y hardware.
b. procedimientos para determinar si algo ha puesto en peligro los activos (pérdida o modificación de los datos).
c. controles para asegurar la devolución o destrucción de la información y activos al final de, o en un punto acordado en el tiempo durante el contrato.
d. integridad y disponibilidad.
e. restricciones sobre la copia y divulgación de información.

- Provisión para la transferencia de personal cuando sea apropiado.
- Las respectivas obligaciones de las partes durante el contrato.
- Las responsabilidades con respecto a temas legales.
- Acuerdos de control de acceso:
- métodos de acceso permitido, y el control y uso de identificadores singulares como IDs y claves secretas de usuarios,
    a. un proceso de autorización para el acceso y privilegios de los usuarios.
    b. un requerimiento para mantener una lista de las personas autorizadas a los servicios disponibles y sobre cuáles son sus derechos y privilegios con respecto a dicho uso.
- La identificación de criterios de desempeño verificables, su monitoreo y reporte;
- El establecimiento de un proceso de intensificación para la solución de problemas; cuando sea apropiado se deberían considerar acuerdos para contingencias
- Responsabilidades relacionadas con la instalación y mantenimiento de hardware
- Una clara estructura de reporte y formatos de reporte establecidos
- Un proceso claro y especificado para la gestión de cambio.

- Capacitación del usuario y el administrador en los métodos, procedimientos y seguridad
- Controles para asegurar la protección contra el software malicioso
- Acuerdos para el reporte, notificación e investigación de incidentes de seguridad y violaciones en la seguridad.

Sistemas de oficina electrónicos

Los Sistemas de oficina electrónicos proporcionan oportunidades para una difusión e intercambio más rápido de la información comercial utilizando una combinación de documentos computadoras computación móvil, comunicaciones móviles correo de voz, comunicaciones de voz en general, multimedia, servició medios postales y máquinas de fax, es por esto que se debe preparar e implementar políticas y lineamientos para controlar los riesgos comerciales y de seguridad.

- Controlar las vulnerabilidades de la información en los sistemas de oficina (grabación de las llamadas telefónicas o conferencias telefónicas, confidencialidad de las llamadas, archivo de faxes) (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*
- Controlar el manejo del intercambio de información (el uso de boletines electrónicos corporativos) (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*
- Restringir el acceso a la información diaria relacionada con personas seleccionadas (personal que trabaja en proyectos confidenciales). (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*
- Restringir los medios seleccionados a categorías de usuarios específicos. (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*

- Retención y backup de la información mantenida en el sistema. (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*

4.1.3.- Área Aplicaciones

4.1.3.1.- Políticas y Estándares de Seguridad

Políticas para el manejo de la Información

Debilidades en la seguridad

Requerir que los usuarios de los servicios de información noten y reporten cualquier debilidad de seguridad observada o sospechada, o las amenazas, en los sistemas o servicios, indicando a su jefe inmediato. *(Norma ISO 17799 - 6.3.2 Reporte de debilidades en la seguridad)*

Mal funcionamiento del software

Establecer los procedimientos para reportar cualquier mal funcionamiento en el software. Considerando las siguientes acciones:

- Anotar los síntomas del problema y cualquier mensaje que aparezca en la pantalla. *(Norma ISO 17799 - 6.3.3 Reporte de mal funcionamiento del software)*
- Detener el uso de la computadora. Si se va a examinar el equipo, debiera ser desconectado de las redes Institucionales antes de volverlo a encender. Los disquetes no debieran ser transferidos a otras computadoras. (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*
- Reportar inmediatamente el problema al encargado de la seguridad de la información. (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*

- Prohibir a los usuarios que no eliminen el software en sospecha a no ser que se le autorice a eso. El personal apropiadamente capacitado y experimentado debiera llevar a cabo la recuperación. (*Norma ISO 17799 - 8.7.5 Seguridad de los sistemas de oficina electrónicos)*

Instalación de aplicaciones

- Las licencias de todo el software que usa la COGMAR deberán ser entregadas al Centro Tecnológico el que será el encargado de la administración y custodia de las mismas. *(PETI)*
- La instalación del software y parches está a cargo de la división de mantenimiento de los Centros Tecnológicos, ellos serán los únicos autorizados a instalar software en las diferentes estaciones de trabajo de la COGMAR a mas de los administradores de red, adicionalmente se restringe al usuario el acceso al disco donde reside el sistema operativo. *(PETI)*
- Queda prohibido instalar copias de software pirata, puesto que además de transgredir la ley de propiedad intelectual, marcas y patentes, pueden contener virus, spyware (software que espía la máquina atacada), archivos de sistema incompatibles con los del usuario, lo cual puede provocar su inestabilidad y fallas en el equipo. *(PETI)*
- Actualizar los Sistemas Operativos Windows 9x de las estaciones de trabajo por razones de seguridad. *(Análisis de la Situación actual)*

Compartir carpetas y archivos

Uno de los métodos mas difundidos por los últimos ataques de virus es el de infectar las máquinas replicándose a si mismos en las carpetas compartidas, dentro de una red. Por lo que los usuarios deben tomar las medidas siguientes:

- Si un usuario debe compartir una carpeta con otro o varios usuarios, esa carpeta debe tener una clave de acceso, la misma que deberá ser cambiada periódicamente. Especificando que usuarios comparte la misma. *(PETI)*
- Luego de que no se requiera más el compartir el recurso en cuestión debe deshabilitarse la opción de compartir dicha carpeta. *(PETI)*

Desarrollo de Aplicaciones

- En el proceso de desarrollo de las aplicaciones se debe seguir una metodología y métricas estándar de desarrollo aprobada y analizada de acuerdo a los requerimientos de la Institución. *(Análisis de la situación actual)*
- Verificar la consistencia de los datos utilizados por las aplicaciones generadas realizando pruebas, antes de su implementación. *(Análisis de la situación actual)*
- Implementar controles dentro del desarrollo de aplicaciones para evitar la fuga o robo de información. *(Análisis de la situación actual)*
- Realizar la documentación de la aplicación (fecha de implementación, analista y programador responsable, objetivos, diagramas de flujo, archivos de entrada- salida que se utiliza y el manual de usuario) para posteriores análisis, cambios o mantenimiento del mismo. *(Análisis de la situación actual)*
- En el caso de que existiera la participación de terceros en el desarrollo de la aplicación el código fuente como la información utilizada para el mismo debe regirse a las norma impuestas por la Institución. *(Análisis de la situación actual)*

4.1.4.- Área Comunicaciones

4.1.4.1.- Políticas y Estándares de Seguridad

Políticas para Control de Acceso a la Red

Uso de los servicios de la red

Las conexiones inseguras a los servicios en red pueden afectar a toda la Institución, sólo se debiera proporcionar a los usuarios acceso directo a los servicios que se le ha autorizados utilizar específicamente.

- Realizar procedimientos de autorización para determinar quién está autorizado a tener acceso a qué redes y servicios en red. *(Norma ISO 17799 - 9.4.1 Política sobre el uso de los servicios en red)*

Terminal de usuario al servicio de cómputo

La ruta desde la terminal del usuario al servicio de cómputo necesita ser controlada para evitar el acceso y uso no autorizado de los medios de información. Podemos reducir dichos riesgos incorporando controles que restringen la ruta entre la terminal del usuario y los servicios de cómputo a los cuales el usuario está autorizado a ingresar.

- Asignar líneas o número telefónicos dedicados. *(Norma ISO 17799 - 9.4.2 Ruta obligatoria)*
- Evitar el recorrido ilimitado en la red. *(Norma ISO 17799 - 9.4.2 Ruta obligatoria)*
- Hacer cumplir el uso de sistemas de aplicación y/o puertas de seguridad especificados para los usuarios de redes externas. *(Norma ISO 17799 - 9.4.2 Ruta obligatoria)*
- Controlar activamente las comunicaciones fuente a destino permitido vía seguridad. *(Norma ISO 17799 - 9.4.2 Ruta obligatoria)*

- Restringir el acceso a la red estableciendo dominios lógicos separados, como redes privadas virtuales para grupos de usuarios dentro de la Institución. *(Norma ISO 17799 - 9.4.2 Ruta obligatoria)*

Segregación en redes

Segregar la red principal en dominios de red lógicos separados por los dominios internos de la Institución y los dominios de red externos, cada uno protegido por un perímetro de seguridad definido (firewalls físicos y lógicos) tomando en cuenta la visión de crecimiento de la red y a la vez separados por servicios de información y usuarios. *(Norma ISO 17799 - 9.4.6 Segregación en redes)*

Control de conexión en red

- Realizar controles de acceso para redes compartidas restringiendo la capacidad de conexión de los usuarios, en aplicaciones como: *(Norma ISO 17799 - 9.4.7 Control de conexión en red)*
    - correo electrónico
    - transferencia de archivos en un solo sentido
    - transferencia de archivos en ambos sentidos
    - acceso interactivo
    - acceso a la red vinculado a la hora del día o fecha.
- Identificar los puntos físicos de voz y datos, comprobar su validez y etiquetarlos para el control y mantenimiento de los puntos de red. *(Análisis de la Situación Actual)*
- Realizar pruebas periódicas de los puertos de red para verificar si permanecen habilitados o no de acuerdo a las normas establecidas. *(Análisis de la Situación Actual)*

- Realizar un análisis para la implementación de un canal de backup de las diferentes redes en caso de emergencia. *(Análisis de la Situación Actual)*

Políticas de acceso al Internet

Uso del Internet

- El servicio de Internet de la COGMAR está dirigido a ciertos usuarios de la red que por su cargo o función necesitan de este servicio y comprende indistintamente tanto a los señores oficiales, tripulantes o empleados civiles. *(PETI)*
- Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP. *(PETI)*
- Habilitar el uso del Chat externo a usuarios autorizados. *(Análisis de la Situación Actual)*
- No contestar los mensajes SPAM, ya que al hacerlo se re-configurará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc. *(PETI)*
- Borre constantemente los cookies, archivos temporales e historial del Internet, con la opción Herramientas, Opciones de Internet, de su navegador. *(PETI)*

Software Malicioso

La protección contra software malicioso se debiera basar en la conciencia de seguridad, acceso apropiado al sistema mediante controles de detección y prevención.

- Indicar medidas de protección de los riesgos asociados al obtener archivos y software, ya sea desde o vía redes externas. *(Norma ISO 17799 - 8.3.1 Controles contra el software malicioso)*

- Instalar y actualizar software anti-virus y de reparación para analizar las computadoras y medios, ya sea como un control de precaución o de manera rutinaria. *(Norma ISO 17799 - 8.3.1 Controles contra el software malicioso)*
- Realizar revisiones regulares del software y el contenido de los datos de los sistemas que sostienen los procesos críticos. *(Norma ISO 17799 - 8.3.1 Controles contra el software malicioso)*
- Chequear antes de usar cualquier archivo en los medios electrónicos de origen incierto o no autorizado o los archivos recibidos a través de redes no confiables, para verificar si tienen virus. *(Norma ISO 17799 - 8.3.1 Controles contra el software malicioso)*
- Chequear antes de usar cualquier archivo adjunto en el correo electrónico y las descargas para ver si tienen algún software malicioso. *(Norma ISO 17799 - 8.3.1 Controles contra el software malicioso)*
- Realizar procedimientos para lidiar con la protección contra virus en los sistemas (recuperación de ataques de virus). *(Norma ISO 17799 - 8.3.1 Controles contra el software malicioso)*
- En caso de recibir un mensaje bajo sospecha de virus, debe contactarse con su área de soporte técnico o con el administrador de la red. *(Análisis de la Situación Actual)*

Antivirus

- El administrador del antivirus debe configurar al antivirus corporativo para rastrear toda la red permanentemente. En la configuración deben constar el rastreo de los discos duros de las máquinas, los disquetes, los archivos de correo adjunto, archivos descargados de la web, etc. *(PETI)*

- Realizar el monitoreo diario de los servidores y estaciones de trabajo, los usuarios y las versiones de software antivirus instalado en cada uno de ellos para actualizar el antivirus a los equipos que no se encuentren con el software actualizado o detectar posibles infecciones y acciones inmediatas a tomar. *(PETI)*

Correo Electrónico

La Institución debe controlar en el uso del correo electrónico:

- ataques por correo electrónico (virus, intercepción). *(Norma ISO 17799 - 8.7.4.2 Políticas sobre correo electrónicos)*
- protección de los archivos adjuntos del correo electrónico. *(Norma ISO 17799 - 8.7.4.2 Políticas sobre correo electrónicos)*
- responsabilidad del empleado de no comprometer a la Institución (enviando un correo electrónico difamatorio, utilizándolo para hostigamiento, compras no autorizadas). *(Norma ISO 17799 - 8.7.4.2 Políticas sobre correo electrónicos)*
- uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (firmas digitales). *(Norma ISO 17799 - 8.7.4.2 Políticas sobre correo electrónicos)*
- retención de mensajes que, si se guardan pueden ser descubiertos en caso de litigio. *(Norma ISO 17799 - 8.7.4.2 Políticas sobre correo electrónicos)*
- controles adicionales para analizar los mensajes que no pueden ser autenticados. *(Norma ISO 17799 - 8.7.4.2 Políticas sobre correo electrónicos)*
- No descargar archivos con extensión .exe, .vbs, avi, protectores de pantalla, etc. que no provengan de un usuario conocido. En estos casos, se les recomienda borrar inmediatamente el mensaje sin abrirlo y de ser detectados por el administrador serán borrados desde el servidor. *(PETI)*

Capítulo 5. Elaboración del Manual de Seguridad Informática

5.1.- Estructura, formato y documentación del Manual de Seguridad Informática

La estructura y formato del Manual de Seguridad Informática estará basado en la Guía para la elaboración de Manuales de la Armada del Ecuador, y a su vez dirigida al personal de la misma para la aplicación de la Seguridad Informática dentro de sus instalaciones. Es de destacar que la información contenida en el manual fue analizada y aprobada por la Dirección Desarrollo Administrativo e Informático (DIRDAI) por lo que es de uso exclusivo de la Institución.

El Manual de Seguridades Informáticas tendrá los siguientes contenidos:

- Carátula
- Presentación
- Índice
- Capítulo I (Objetivos, Distribución, Difusión, Alcance y Uso del Manual)
- Capítulo II (Generalidades del Manual)
- Capítulo III (Políticas de la Seguridad Informática)

La versión final del Manual de Seguridad Informáticas fue entregada a la Dirección Desarrollo Administrativo e Informático (DIRDAI) y por motivos de ser una Institución militar se solicitará que se mantenga como reservada el proyecto de tesis.

Capítulo 6. Conclusiones y Recomendaciones

6.1.- Conclusiones

- Las facilidades de trabajo proporcionado por la Dirección Desarrollo Administrativo e Informático hicieron posible el cumplimiento de los objetivos planteados en el proyecto de tesis.

- Para este trabajo se utilizaron varias metodologías de análisis de riesgos obteniendo una propuesta final que se encuentra planteada en el proyecto de tesis.

- Para el planteamiento de las políticas informáticas se uso como base principal la norma ISO/IEC 17799 correspondiente a la Tecnología de Información – Código de Práctica para la Gestión de la Seguridad de la Información.

- Se tomo también como referencia principal los manuales organizacionales, planes estratégicos, norma y políticas Institucionales.

- Es importante de destacar que la elaboración del Manual de Seguridad Informáticas se fundamento en las variables de seguridad: Confidencialidad, Integridad, Disponibilidad, Autenticación, No-Repudio.

- Mediante la aplicabilidad del Manual presentado, la Armada del Ecuador podrá aplicar procedimientos y controles basados en las políticas expuestas, y con ello asegurar la integridad de sus activos informáticos.

6.2.- Recomendaciones

- Se recomienda hacer un énfasis en el tema de concientización Institucional ya que es una de las bases principales para el desarrollo de la seguridad informática.

- Se recomienda analizar cada una de las políticas presentadas para visualizar el impacto que puede ocasionar a la Institución en el caso de no aplicarlas.

- Se recomienda la estandarización de ambos Centros Tecnológicos tanto en hardware, software y como en políticas de seguridades informáticas para evitar el desequilibrio de las actividades, denegando así los controles para el correcto desenvolvimiento de la Institución.

- Se recomienda dar a conocer el contenido de los Planes de Contingencia y Políticas de Seguridad Informáticas.

- Se recomienda que una vez implementado las políticas propuesta realizar un nuevo análisis de riesgos para verificar si el porcentaje de las vulnerabilidades se ha disminuido o aumentado y con ello tomar medidas en el asunto.

Bibliografía

- Plan Estratégico de las Tecnologías de la Información de la Armada Del Ecuador

- Manual Organizacional de la Armada del Ecuador

- Manual Organizacional de la Dirección Desarrollo Administrativo e Informático

- Situación Tecnológica Actual de la Fuerza Naval

- Norma ISO/IEC 17799 “Tecnología de Información – Código de Práctica para la Gestión de la Seguridad de la Información”

- INEI - Plan De Contingencias y Seguridad de la INFO /29
  http://www.inei.gob.pe/web/metodologias/attach/lib611/0300.HTM

- Seguridad de la Información: Un nuevo enfoque para el control de riesgos de negocio PC-NEWS.COM
  http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=1926

- Estándares De Seguridad En La Información
  http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

- Implantación de la Norma de Seguridad ISO 17799
  http://www.s21sec.com/s21sec/ser_iso.jsp

- Métodos y seguridad de un sistema de información

  http://www.ssi.gouv.fr/es/confianza/documents/bs7799-es.html

- Gestión de Seguridad de la Información

  http://www.dnv.com.ar/certificacion/sistemasdegestion/seguridaddelainformacion/descripcion.asp

- Implantación Voluntaria De Sistemas De Gestión De La Seguridad En La Información (SGSI)

  http://www.burotec.es/seg_info_03.htm

ANEXO A

Cuestionarios Aplicados

SEGURIDAD LÓGICA

Nombre:..... **Cargo: .....**

Departamento: …..... **Fecha:.....**

Identificación de usuarios

¿Para el control de la seguridad qué datos son almacenados en el perfil de usuario?

☐ ID de usuario

☐ Nombre y apellido completo

☐ Puesto de trabajo y departamento de la Institución

☐ Tipo de cuenta o grupo al que pertenece (empleado, director, etc)

☐ Fecha de expiración de la cuenta

☐ Datos de los permisos de acceso y excepciones

¿El ID del usuario puede repetirse?

SI ☐ NO ☐

Mantenimiento

¿Se actualizan, revisan y asignan a los usuarios un grupo determinado con sus respectivos permisos?

SI ☐ NO ☐

¿Cada cuánto tiempo?

☐ 1 a 3 meses ☐ 4 a 6 meses ☐ 7 o más ☐ Cada vez que se requiera

Permisos

La clasificación de los recursos (datos) esta basado por:

☐ Importancia

☐ Los tipos (base de datos, archivos de configuración, datos personales)

☐ Por departamento

¿Quiénes son los encargados de asignar permisos a los usuarios?

☐ Administrador ☐ Usuarios privilegiados ☐ Director

ID Inactivas

¿Después de un período de inactividad en que el usuario no realiza acciones en el sistema o en la Pc?

☐ Se limpia la pantalla asociada al usuario

☐ Se desconecta el usuario inactivo

☐ Pide la contraseña de nuevo

Acciones correlativas a usuarios

¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan?

SI ☐ NO ☐

¿Se generan históricos de las actividades de los usuarios en el sistema?

SI ☐ NO ☐

Grupos- Roles

¿Cómo se forman los grupos de usuarios?

☐ Según el departamento de la Institución donde trabajen

☐ Según el rol que desempeñen

¿Se eliminan los usuarios que vienen por default en el sistema operativo?

SI ☐ NO ☐

Súper usuario

¿Qué tipos de perfil de administración hay?

☐ Administrador de Bases de Datos Cuántos.……

☐ Administrador de Redes y Comunicaciones Cuántos…….

☐ Administrador de Aplicaciones Cuántos……

¿Desde qué terminal puede autenticarse un administrador?

☐ Pc de cualquier usuario ☐ Servidores

¿Qué datos se muestran cuando alguien intenta autenticarse?

☐ Nombre de usuario ☐ Password ☐ Grupo o entorno de red

☐ Estación de trabajo ☐ Fecha y hora

¿Qué datos se almacenan cuando alguien logra autenticarse?

☐ Fecha y hora de la última conexión ☐ Localización de la última conexión

¿Utilizan el ID de usuario como:

☐ Control de acceso a los recursos ☐ Solo para ingreso al sistema

Autenticación

¿Qué se muestra en pantalla cuando se escribe la contraseña de ingreso a la red?

☐ Espacios ☐ Asteriscos ☐ No se mueve el cursor

¿Cómo se guardan las claves de autenticación en disco (servidores)?

☐ Encriptados ☐ Se visualiza la clave

¿Se clasifica como confidencial a los datos de autenticación?

SI ☐ NO ☐

¿Quién tiene acceso a los datos de autenticación?

☐ Usuarios ☐ Administrador de Red y Comunicaciones

☐ Administrador de Base de Datos ☐ Administrador de Aplicaciones

La autenticación es:

☐ Para una aplicación en particular ☐ Para toda la red

☐ Para la red LAN ☐ Para la red WAN

¿Cuándo un usuario se autentifica de forma errónea:

☐ Se bloquea el usuario después de varios fallidos de autenticación
☐ Se inhabilita la cuenta o la terminal

¿Después de cuantos intentos?

☐ 1 a 3 ☐ 5 o más

¿Se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos o para mensajes externos?

SI ☐ NO ☐

¿Qué ocurre con la cuenta del administrador en el período de vacaciones?

☐ Se bloquea la cuenta

☐ Hay otra persona que tiene los mismos permisos del administrador principal

☐ Se revela las contraseñas y procedimientos a una persona de confianza

¿Se procede de igual manera que el caso anterior con el resto de los usuarios?

SI ☐ NO ☐

Contraseñas

¿Las contraseñas son creadas:

☐ Por procesos automáticos (programas de generación de contraseña)

☐ Por los usuarios

¿Cuál es el conjunto de caracteres permitidos para la contraseña:

☐ Alfa-Numéricos ☐ Numéricos ☐ Caracteres especiales

¿Cuál es el largo mínimo y máximo de caracteres para la contraseña?

☐ 1-5 caracteres ☐ 6-8 caracteres

¿La contraseña se inicializa como expirada cuando el usuario ingresa por primera vez al sistema o a la red?

SI ☐ NO ☐

¿Se permite al usuario autenticarse a pesar de que su contraseña ha expirado?

SI ☐ NO ☐

Si existe más de una cuenta de administrador, ¿algunas de estas (o todas) tienen las mismas contraseñas?

SI ☐ NO ☐

¿En que periodo de tiempo se cambia la contraseña?

☐ Cada 15 días ☐ Cada Mes

¿Se puede cambiar en cualquier momento el passwords de los usuarios?

SI ☐ NO ☐

¿Quién puede hacer los cambios de los password?

☐ El administrador de Redes y Comunicaciones

☐ Los usuarios a través de una opción en el menú

☐ Otros Administradores

¿Se guarda en una base de datos con las últimas password de los usuarios?

SI ☐ NO ☐

Entrenamiento a usuarios

¿Se entrena a los usuarios en la administración del password? ¿Se les enseña a:

☐ No usar passwords fáciles de descifrar?

☐ No divulgarlas?

☐ No guardarlas en lugares donde se puedan encontrar?

Control De Acceso Lógico

¿Para el control de acceso usan una aplicación como (Active Directory)?

SI ☐ NO ☐

¿Si su respuesta es Negativa qué herramienta utiliza?

……

¿Esta aplicación es:

☐ Propia del sistema operativo

☐ De aplicación y programas propios o comprados

☐ Con paquetes de seguridad agregados al sistema operativo

Limitaciones a los servicios

¿Existen restricciones de servicio en base a:

☐ Usuarios ☐ Aplicaciones ☐ Departamentos

Mecanismos de control de acceso interno

¿Se restringen las interfaces que ven los usuarios, (como el escritorio de Windows) de manera que los usuarios solo vean lo que les está permitido?

SI ☐ NO ☐

¿Se encriptan algunos datos, cuales:

☐ Los mensajes

☐ Las passwords y datos de las cuentas de usuarios

☐ Los datos de configuración

☐ Los datos críticos de la organización

Control de acceso externo
Existen mecanismos de control de acceso externo:

☐ Gateways (puertas de seguridad) o firewalls seguros

☐ Acceso de personal contratado, consultores o mantenimiento

☐ Autenticación basada en host: ¿existe una autenticación que da acceso al sistema basándose en la identidad del host que pide el acceso, y no en la identidad del usuario que quiere entrar?

¿Existe acceso externo a los datos, desde Internet?

SI ☐ NO ☐

¿Se tienen en cuenta los siguientes procedimientos para mantener la integridad y la confiabilidad de los datos?

☐ Control de acceso para limitar lo que se lee, ve, borra, modifica, etc.

☐ Firmas digitales

☐ Ponen las copias de seguridad de la información pública, en otro lado, no en la misma máquina

☐ Prohíben el acceso público a bases de datos

☐ Verifican que los programas y la información pública no tenga virus

☐ Están separados los datos que se publican en Internet de los datos del interior de la empresa

Sistema De Detección De Intrusos (Ids)
¿Se usan herramientas de monitorización de red para encontrar intrusos?

SI ☐ NO ☐

Si hubiera una entrada de un intruso:

☐ Se documenta

☐ Se documenta y se da seguimiento correctivo

☐ Se documenta, se da seguimiento correctivo, se verifica que implicaciones pudo tener en la empresa

¿Usan herramientas para detectar cambios en la configuración o en los archivos?

SI ☐ NO ☐

Firma: …….

SEGURIDAD FÍSICA

Nombre:..... **Cargo: .....**

Departamento: …..... **Fecha:.....**

Control de acceso al Centro de Cómputos

¿Se restringe el acceso al centro de cómputos a la gente que no pertenece a esa área?

Si ☐ No ☐

¿Existen algunos de los siguientes métodos? ¿Dónde?

- ☐ Tarjetas de entradas,
- ☐ Guardias de Seguridad,
- ☐ Llaves Cifradas (Looked Door),
- ☐ Circuito cerrado de televisión.

Control De Acceso A Equipos

¿La BIOS tiene habilitada una contraseña?

Si ☐ No ☐

¿Las PC's tienen habilitados los dispositivos externos, como la disquetera o a lectora de CD?

Si ☐ No ☐

¿Se controlan los virus en las disqueteras o CD's?

Si ☐ No ☐

¿Lo realizan mediante la configuración del Antivirus al ingresar un disquete?

Si ☐ No ☐

¿Se permite desde el setup de la máquina el booteo con CD`s o disquetes)?

Si ☐ No ☐

¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados?

Si ☐ No ☐

¿Puede alguien enchufar e instalar una impresora u otro dispositivo (un zip o un disco removible) en alguna máquina?

Si ☐ No ☐

¿Se mantienen prendidos los servidores las 24 horas?

Si ☐ No ☐

¿Cada cuánto tiempo se reinician?

☐ Diario ☐ Semanal ☐ Quincenal

Utilidades de soporte

¿Existen, se mantienen y revisan todos estos aparatos periódicamente en busca de fallas?

☐ Aire acondicionado (18º C a 20º C) ☐ Calefacción

☐ Luz de emergencia en el centro de cómputos ☐ Detectores de humo, agua y calor

¿Disponen UPS (Uninterruptible power supply) para mantener funcionando todas las máquinas necesarias para el trabajo diario? Si ☐ No ☐

¿Se han probado los UPS trabajando al 100% de necesidad para probar su correcto funcionamiento? Si ☐ No ☐

¿Disponen de extintores de incendio? Si ☐ No ☐

¿Se ha entrenado al personal en la utilización de los extintores? Si ☐ No ☐

¿Los extintores se encuentran en lugares visibles y de fácil acceso? Si ☐ No ☐

¿Disponen de rociadores? Si ☐ No ☐

¿Se revisan las posibles fallas eléctricas o posibles causas de incendio? Si ☐ No ☐

¿Las máquinas tienen alguna protección de agua cuando cae la lluvia artificial? Si ☐ No ☐

¿Hay un dispositivo que evite la sobrecarga de la red eléctrica? Si ☐ No ☐

Estructura Del Edificio

¿Se tuvo en cuenta la seguridad de los datos y equipos en el momento de hacer la estructura de los edificios? Si ☐ No ☐

Centro de cómputos:

¿El Centro de Cómputo está ubicado en pisos elevados (para prevenir inundaciones)? Si ☐ No ☐

¿Existe un piso o techo falso para pasar el cableado por debajo de él?

Si ☐ No ☐

¿Es lo suficientemente grande, anticipándose al crecimiento de la red y predispuesto a reinstalaciones?

Si ☐ No ☐

¿El Centro de Cómputo está en el mismo lugar del backbone central de la red?

Si ☐ No ☐

¿Esta permitido comer, fumar y beber dentro del centro de cómputos?

Si ☐ No ☐

Cableado

¿Usan cableado estructurado basándose en una norma?

Si ☐ No ☐

¿Se tuvo en cuenta el lugar de los canales de red, de manera que no sean afectados por desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos?

Si ☐ No ☐

¿Existe un interruptor de energía de emergencia en la puerta de salida?

Si ☐ No ☐

Interceptación física, visual y electromagnética

¿Puede haber emisiones electromagnéticas desde los monitores o desde los cables UTP, que se pueden interceptar o provocar ruidos?

Si ☐ No ☐

Sistemas Móviles

¿Si se usan laptops o PC's portátiles, se tienen en cuenta los diferentes riesgos a los que se someten los datos de la empresa?

Si ☐ No ☐

Clasificación de datos y hardware

¿Existen procesos para rotular, manipular y dar de baja la computadora, sus periféricos y medios de almacenamiento removibles y no removibles?

Si ☐ No ☐

Backup

¿Con qué frecuencia hacen los backups?

☐ Diarios ☐ Semanales ☐ Quincenales

Backups del Hardware.

Modalidad externa: ¿contratan un tercero que proporcione los insumos necesarios en caso de emergencia?

Si ☐ No ☐

Modalidad interna: si tienen más de un local, en ambos locales deben tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local. ¿Se realizan estas actividades en la empresa?

Si ☐ No ☐

¿Hay herramientas de back up automáticas, o sea que a través de una agenda hacen las copias?

Si ☐ No ☐

¿Existen prioridades en las PC's (ej. Se saca respaldo de las máquina de los Directores)?

Si ☐ No ☐

¿Los backups se almacenan dentro y fuera del edificio en lugares seguros?

Si ☐ No ☐

¿Guardan las cintas de backup en?

☐ Banco ☐ Caja Fuerte en el mismo departamento

☐ Otros……..

¿Se necesita algún dispositivo (llaves, tarjeta) para entrar al almacén de cintas?

Si ☐ No ☐

¿Hay información afuera de la red interna de la empresa que sea valiosa?

Si ☐ No ☐

¿Hay backups de las páginas Web y de sus actualizaciones?

Si ☐ No ☐

Firma: ……..…….

PLAN DE CONTINGENCIAS

Nombre:..... **Cargo: .....**

Departamento: …..... **Fecha:.....**

¿Existe un plan de contingencias?

Si ☐ No ☐

¿Se desarrolló un previo análisis de riesgo antes de realizar el plan de contingencias?

Si ☐ No ☐

¿El plan de contingencias se desarrolló en base a:

☐ Al área de cómputos, o

☐ Se tuvieron en cuenta otras áreas de la empresa

¿El plan de contingencias incluye un Plan de recuperación de desastres?

Si ☐ No ☐

¿El plan de contingencias incluye un Plan de reducción de riesgos?

Si ☐ No ☐

¿Se definen las responsabilidades y funciones de las personas en el plan de contingencias?

Si ☐ No ☐

¿Poseen las acciones defensivas en caso de violación interna o externa? (Ej. desconectar los servidores, cerrar los accesos, rastrear al intruso, etc.),

Si ☐ No ☐

¿Hay algún tipo de mecanismo de reportes o historial, para el manejo de incidentes?

Si ☐ No ☐

¿Se mantiene actualizado el Plan de Contingencias de acuerdo a nuevos puestos y funciones, o amenazas?

Si ☐ No ☐

Centro de Cómputo Alternativo

¿Existe un CPD alternativo que cumpla con las mismas funciones que el principal?

Si ☐ No ☐

Plan De Recuperación De Desastres

¿En el caso de que haya un plan de recuperación de desastres, cada miembro del equipo tiene una responsabilidad asignada?

Si ☐ No ☐

¿Se dividen las acciones correctivas en equipos de trabajo?

Si ☐ No ☐

¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia?

Si ☐ No ☐

Antes Del Desastre

Identificación de las funciones críticas.

¿Existe una lista de datos, elementos de hardware y software críticos a proteger en la organización, en el momento de un desastre?

Si ☐ No ☐

Constitución del grupo de desarrollo del plan.

¿El Director es el responsable de la implementación del plan de emergencias?

Si ☐ No ☐

¿Si su respuesta es Negativa Quien es el responsable?

……..

Sistemas de información:

¿Están identificados todos los sistemas de información y sus características (como si fuera un inventario de los sistemas)?

Si ☐ No ☐

¿Qué datos se almacenan de los sistemas?

☐ Nombre

☐ Lenguaje

☐ Departamento de la empresa que genera la información

☐ Departamentos de la empresa que usan la información

☐ El nivel de importancia estratégica que tiene la información de este Sistema para la Institución

☐ Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando

Equipos de cómputos:

¿Si se mantiene un inventario de los equipos de cómputos? Se incluye:

- ☐ Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.
- ☐ Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
- ☐ Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivados fuera de línea, backup, bases de datos, dueño designado de la información.
- ☐ Configuración de los equipos (y sus archivos de configuración).
- ☐ Ubicación de los equipos y de los datos.

¿Existen pólizas de seguros para los equipos en el caso de siniestros?

Si ☐ No ☐

Backup:

¿Existen procedimientos para realizar back up en el caso de una emergencia?

Si ☐ No ☐

¿Están incluidos en el plan de contingencia?

Si ☐ No ☐

¿Se realizan simulacros en base al Plan de Contingencia?

Si ☐ No ☐

¿Cada cuánto lo realizan?

☐ 3 meses ☐ 6 meses ☐ 9 meses

¿Cada cuanto tiempo se da a conocer el Plan de Contingencias, sea nuevo o modificado, al personal de la institución?

☐ 3 meses ☐ 6 meses ☐ 9 meses

Durante El Desastre

¿Poseen un plan de emergencia (consiste de las acciones a llevar a cabo durante el siniestro)?

Si ☐ No ☐

¿Se tienen en cuenta los distintos escenarios posibles?

Si ☐ No ☐

¿Se incluyen los siguientes puntos?:

☐ ¿Vías de salida?

☐ ¿Plan de evacuación del personal?

☐ ¿Plan de puesta a buen recaudo de los activos?

☐ ¿Ubicación y señalización de los elementos contra el siniestro?

Después Del Desastre

Evaluación de Daños: ¿se realizan las siguientes actividades después de que ha ocurrido algún desastre?

☐ ¿Evalúan la magnitud del daño que se ha producido?

☐ ¿Que sistemas se están afectando?

Firma: ……..

Administración Del Centro De Cómputos (CPD)

Nombre:..... **Cargo: .....**

Departamento: …..... **Fecha:.....**

¿Se realizan los siguientes chequeos en el sistema?

☐ ¿Extraen un logístico sobre las conexiones de red levantadas?

☐ ¿Extraen un logístico sobre los intentos de ingresos desde el exterior a la red interna?

☐ ¿Extraen un logístico con las conexiones externas realizadas desde la red?

☐ ¿Obtienen un logístico sobre los downloads de archivos realizados y quién los realizó?

¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?

Si ☐ No ☐

¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información?

Si ☐ No ☐

¿Existe documentación detallada sobre el equipamiento informático? Incluye los siguientes datos:

☐ Distribución física de las instalaciones (identificación de PC´s y equipos, y puesto de trabajo)

☐ Inventario de "hardware" y "software" de base

¿Se actualiza la lista de activos?

Si ☐ No ☐

¿Existe algún manual de seguridad, para el personal de seguridad o para los usuarios?

☐ Trusted Facility Manual: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.

☐ Security Features User's guide: asiste a los usuarios del sistema, describe como usar las protecciones, las responsabilidades de la seguridad del sistema.

R**esponsabilidad Del Equipo De Seguridad**

¿Existe un solo responsable del centro de cómputo?

Si ☐ No ☐

¿Se le informa al director sobre la administración de seguridad, actividad de seguridad de la información, y riesgos?

Si ☐ No ☐

¿Existe en los empleados y el director una conciencia sobre su importancia de la seguridad?

Si ☐ No ☐

Firma: ……

DESARROLLO DE LAS APLICACIONES

Nombre:..... **Cargo: .....**

Departamento: …..... **Fecha:.....**

Ciclo De Vida

¿Se desarrollan aplicaciones para cada área de la Institución?

Si ☐ No ☐

¿Usan alguna metodología estándar para el desarrollo de sistemas?

Si ☐ No ☐

¿Usan mecanismos de seguridad durante las fases de desarrollo?

Si ☐ No ☐

Iniciación

¿Se expresan los requerimientos del sistema?

Si ☐ No ☐

Desarrollo

¿Se hace un análisis de riesgos antes de empezar con el desarrollo?

Si ☐ No ☐

¿En caso de que haya participación de terceros en el desarrollo (como en la web, o en LINUX) el código fuente queda en la Institución?

Si ☐ No ☐

¿Usan métricas durante el desarrollo?

Si ☐ No ☐

¿Se mantienen registros históricos de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento? ¿Qué se guarda?

- ☐ Sistema que afecta,
- ☐ Fecha de la modificación,
- ☐ Persona que realizó el cambio,
- ☐ Descripción global de la modificación,

Implementación

¿Se tienen medidas de seguridad durante la implementación?

Si ☐ No ☐

Prueba

¿Se generan planes de prueba?

Si ☐ No ☐

¿Se documentan las pruebas y sus resultados? Si ☐ No ☐

Instalación y mantenimiento

¿Se realiza mantenimiento en los sistemas? Si ☐ No ☐

Documentación

¿Qué documentación generan de los desarrollos que hacen? ¿Se incluyen las siguientes cosas?

☐ Generalidades del sistema, incluyendo fecha de implementación y analista / programador responsable.

☐ Documentación del sistema, incluyendo sus objetivos, diagramas general y de funciones y diseños de registros.

☐ Documentación de los programas, incluyendo objetivos, diagrama de flujo y archivos de entrada y salida que utiliza.

☐ Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores.

☐ Manual de usuario.

☐ Manual de características de seguridad.

☐ Descripción del hardware y software, políticas, estándares, procedimientos, backup, plan de contingencia, descripción del usuario y del operador del sistema.

Compra

¿Se toman medidas antes de comprar un sistema?

Si ☐ No ☐

¿Existe documentación de los sistemas comprados, así como los vendedores y del soporte postventa?

Si ☐ No ☐

Firma: ……

SEGURIDAD EN LAS COMUNICACIONES

Nombre:..... **Cargo: .....**

Departamento: …..... **Fecha:.....**

Configuración De Red

¿Cómo es la topología de la red?

☐ Anillo ☐ Estrella ☐ Bus ☐ Mixtas

¿Existe un inventario o gráfico topológico de la red que incluye lo siguiente ?

☐ Switch ☐ Routers ☐ Hub's ☐ Modem

☐ PC's ☐ Conexiones de radio ☐ Fibra óptica

Servidor de Hosting

¿Qué se tuvo en cuenta para elegir el servidor de hosting?

☐ Precio

☐ Medidas de seguridad

☐ Respaldo en caso de emergencia, de caída del servidor y de pérdida de info.

Comunicaciones

¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a Internet?

SI ☐ NO ☐

Recursos compartidos

¿Se comparten los discos o carpetas de las PC's en la red

☐ Con permisos a cualquier usuario

☐ Personalizado con sus respectivos permisos a quien necesite

¿Cualquier usuario está permitido a compartir carpetas?

SI ☐ NO ☐

¿Se pueden ver las carpetas de los mails de los otros usuarios?

SI ☐ NO ☐

¿Utiliza algún software para colocar contraseñas a las carpetas?

SI ☐ NO ☐

¿Quién pone las contraseñas:

☐ El dueño de la información ☐ El administrador

Configuración de puertos

¿Se deshabilitan los puertos que no son necesarios?

SI ☐ NO ☐

¿Se prueban los puertos de la red?

SI ☐ NO ☐

¿Se hace algún chequeo periódico de la red y sus permisos?

SI ☐ NO ☐

¿Qué servicios son necesarios para el mantenimiento y desarrollo de la Institución:

☐ HTML ☐ FTP ☐ IP ☐ DNS ☐ TELNET

Medidas de fiabilidad

¿ Existen medios alternativos de transmisión de datos en caso de que exista alguna contingencia con la red?

SI ☐ NO ☐

¿Disponen Servidor de :

☐ Base de Datos ☐ Aplicaciones ☐ Mail ☐ Internet

☐ Dominio ☐ Proxy ☐ Firewall

¿Disponen de Servidor de Backup?

☐ Base de Datos ☐ Aplicaciones ☐ Mail ☐ Internet

☐ Dominio ☐ Proxy ☐ Firewall

Mail – Chat

¿Disponen de un servidor solo para mail?

SI ☐ NO ☐

¿Tienen servicio de correo:

☐ Solo interno ☐ Interno con salida externo y viceversa

¿Pueden revisar el correo

☐ Desde la empresa ☐ Por el Internet

¿Las cuentas de correo nuevas se crean previa autorización? SI ☐ NO ☐

Las claves de autenticación de correo son de conocimiento de

☐ El Administrador de comunicaciones y redes ☐ El Usuario

¿Los mails se borran del servidor cuando son descargados a la máquina del usuario? SI ☐ NO ☐

Espacio en disco

¿Cómo se administra la capacidad de disco asignada a los mails?

☐ ¿Se asigna un espacio de disco a la totalidad del correo?

☐ ¿Se asigna un espacio de disco a cada cuenta de mail?

☐ ¿Se asigna un espacio de disco a cada departamento?

☐ ¿Existen distintas cantidades asignadas a los usuarios de acuerdo a su perfil o grupo, o todos los usuarios tienen la misma cantidad de espacio en disco?

¿Si se mantienen los correos en el servidor tienen alguna herramienta o procedimiento que advierta la falta de espacio en disco? SI ☐ NO ☐

¿Se puede suspender solo su servicio de mail sin afectar el resto de la empresa? SI ☐ NO ☐

¿Restringen el tamaño del correo tanto para el ingreso o salida de correos? SI ☐ NO ☐

¿Existen direcciones de mail para todos los empleados? SI ☐ NO ☐

¿Controlan los SPAMS en estas direcciones? SI ☐ NO ☐

¿Se identifica y administra al correo basura? SI ☐ NO ☐

Chat

¿Se permiten los servicios de chat? SI ☐ NO ☐

¿Cuáles se usan?

☐ MSN ☐ Yahoo ☐ Mensajería de Windows ☐ Jabber

¿Se permite bajar archivos a través de estos programas?

SI ☐ NO ☐

¿Se usan programas de file sharing (Morfeus, Kazaa, Napster, Audio Galaxy, iMesh, eDonkye2000, etc.)?

SI ☐ NO ☐

Privacidad – Firma digital – Encriptación de mails

¿Prohíben el envío de archivos de la empresa u otros documentos confidenciales vía mail?

SI ☐ NO ☐

¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales?

SI ☐ NO ☐

¿ Qué sería importante proteger, en el caso de mensajes internos y externos?:

☐ ¿Integridad? ☐ ¿Confidencialidad?

☐ ¿No repudio? ☐ ¿Autenticación del remitente?

¿Se pide generalmente una confirmación de lectura en los mails salientes?

SI ☐ NO ☐

Virus – Antivirus

¿Cuáles de éstas medidas o herramientas poseen para evitar los virus?

☐ Paquetes de software antivirus

☐ Firewalls

☐ Sistemas de detección de intrusos

☐ Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos.

☐ Creación de un disco de rescate o de emergencia

☐ Procedimientos para cuando ocurra una infección con virus.

☐ Hardware de seguridad de red dedicado

☐ Back up de datos

¿Verifican la existencia de virus en :

☐ Correos entrantes ☐ Correo salientes

¿Existen mecanismos de filtrado que permitan buscar ciertas frases o palabras dentro del encabezado o cuerpo del mensaje, para determinar si hay algún mail con virus o correos no deseados?

SI ☐ NO ☐

¿El antivirus está instalado en cada PC (incluyendo los servidores)?

SI ☐ NO ☐

¿Las actualizaciones de virus se descargan

☐ Cada pc ☐ El servidor para toda la red?

Si se encuentra un mail con virus, ¿qué se hace para que no lleguen más de esa misma persona?

☐ ¿Se identifica la fuente del mail, para bloquearla desde el router o desde el servidor de correo?

☐ ¿Se avisa al ISP para que no deje entrar más mails de esa dirección?

☐ ¿Se observan los encabezados de los mails para identificar su origen verdadero?

¿ Cada cuanto se hace un escaneo total de virus en los servidores?

☐ Semanal ☐ Quincenal ☐ Mensual

¿ El escaneo de las maquinas se realiza por:

☐ Cuenta de cada usuario ☐ El servidor

Documentación

¿Qué documentación existe de la red?

☐ ¿Diagramas topológicos?

☐ ¿Procedimientos?

☐ ¿Manuales?

☐ ¿Certificados (Ej.: de calidad, etc.)?

☐ ¿Licencias de software?

☐ ¿Planes de contingencia, de seguridad, etc.?

☐ ¿Contratos (Ej.: responsabilidades y mecanismos de transmisión al establecer una comunicación con las fábricas)

☐ ¿Cambios realizados en la configuración de la red?

¿Poseen cada uno de estos elementos de documentación de la empresa?

☐ Manual de uso del software y de hardware usado (del software desarrollado y del comprado).

☐ Diagramas de red y documentación de la configuración de routers, switches y dispositivos de red.

☐ Procedimientos de emergencia (plan de contingencia)

☐ Plan de seguridad

☐ Manual de procesos estándares del Sistema Operativo (en especial de Linux)

¿Se han instalado correctamente todos los parches de seguridad disponibles del sistema operativo y de los programas usados? SI ☐ NO ☐

¿Hay alguna documentación donde se anote la configuración de las PC´s en la red (Sus números IP, sus placas de red, etc.)? SI ☐ NO ☐

Ataques De Red

De los siguientes métodos contra los ataques más comunes, ¿qué está implementado?

Denial of service:

☐ ¿Limitan el tráfico de red?

☐ ¿Instalan los parches de seguridad del sistema operativo?

☐ ¿Utilizan alguna herramienta para detectar cambios en la información de configuración u otros archivos (como Tripwire)?

Sniffing:

☐ ¿Las líneas de comunicación se segmentan tanto como sea práctico?

☐ ¿Los datos de logeo y otros datos sensibles son transmitidos encriptados?

Spoofing:

☐ ¿Tienen alguna herramienta anti-spoofing?

☐ ¿Los routers son configurados para que rechacen los ataques de spoofing?

Firewall

¿En que máquina (servidor) se encuentra el Firewall?

☐ Máquina dedicada ☐ En el servidor de Internet?

¿Qué tipo de firewall disponen?

☐ ¿firewall de aplicación diseñado con los requerimientos de la Institución?

☐ ¿firewall de aplicación?

☐ ¿firewall físico (cajas negras)?

☐ ¿firewall de aplicación - físico?

¿Usan una política de acceso a servicios?

Si ☐ No ☐

¿Usan una política de diseño y configuración del firewall? ¿Alguna de estas dos?:

☐ Postura de negación preestablecida: se especifica sólo lo que está permitido y se prohíbe todo lo demás:

☐ Postura de permiso preestablecido: se especifica sólo lo que está prohibido y se permite todo lo demás.

¿Que habilidades tiene para monitorizar la red? Incluye:

☐ ¿Intentos no autorizados de ingreso? ☐ ¿Genera logs?

☐ ¿Provee reportes? ¿O mails? ☐ ¿Tiene alarmas?

¿Puede adaptarse a distintas configuraciones de red o de sistemas (es escalable)?

Si ☐ No ☐

Herramientas Para Administración De Red Y Protocolos

¿Usa alguna herramienta o protocolos para la seguridad de la red?

Si ☐ No ☐

¿Las herramientas que se usan tienen las siguientes funciones?

☐ ¿Pueden monitorear y filtrar peticiones entrantes a distintos servicios?

☐ ¿Indican la hora, la máquina origen (el número de IP) y el puerto de esa conexión?

☐ ¿Pueden seguir una traza de todos los intentos de conexión tanto admitidos como rechazados?

☐ ¿Se monitorea la red buscando ciertos protocolos con actividad inusual?

¿Se llevan estadísticas de uso de los protocolos?

Si ☐ No ☐

¿Se audita el tráfico IP?

Si ☐ No ☐

¿Tienen la posibilidad de filtrar paquetes por hardware o por software?

Si ☐ No ☐

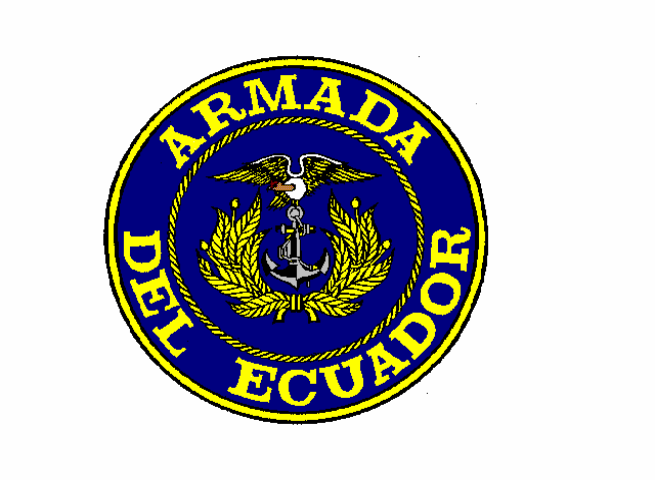
¿Se mantiene actualizado el software de monitoreo?

Si ☐ No ☐

Firma: …….

ANEXO B

Manual de Seguridades Informáticas de la Armada del Ecuador



ESTADO MAYOR DE LA ARMADA

DEPARTAMENTO DE DESARROLLO ADMINISTRATIVO E INFORMÁTICO

QUITO

MANUAL DE SEGURIDADES INFORMÁTICAS

2006

PRESENTACIÓN

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse “a medida”, para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes. De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

Por esta razón, se elaboró un Manual de Seguridades Informáticas que al ser aplicada a una Institución militar se necesita de una concientización y planteamiento de políticas que salvaguarden la confidencialidad de sus activos informáticos, verificando así la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y el cumplimiento de los reglamentos y normas prescriptas.

DEPARTAMENTO DE DESARROLLO ADMINISTRATIVO E INFORMÁTICO
MANUAL DE SEGURIDADES INFORMÁTICAS

ÍNDICE

CAPÍTULO 1

OBJETIVOS, DISTRIBUCIÓN, DIFUSIÓN, ALCANCE Y USO DEL MANUAL

CAPÍTULO II

GENERALIDADES DEL MANUAL

CAPÍTULO III

POLÍTICAS DE SEGURIDAD INFORMÁTICA

CAPÍTULO I

OBJETIVOS, DISTRIBUCIÓN, DIFUSIÓN, ALCANCE Y USO DEL MANUAL

CAPÍTULO I

OBJETIVOS, DISTRIBUCIÓN, DIFUSIÓN, ALCANCE Y USO DEL MANUAL

100 OBJETIVOS

- Resguardar la integridad de los datos y equipos de la Armada del Ecuador.
- Proteger la información contra acciones no éticas que producen la inestabilidad de la Armada del Ecuador.
- Crear una conciencia de seguridad informática a todo el personal militar y civil de la Armada del Ecuador.

200 DISTRIBUCIÓN Y DIFUSIÓN

El Personal de los Centros Tecnológicos del Departamento de Desarrollo Administrativo e Informático será el encargado de la distribución y difusión del Manual de Seguridades Informáticas.

300 ALCANCE Y USOS DEL MANUAL

Personal militar y civil de la Armada del Ecuador.

CAPÍTULO II

GENERALIDADES DEL MANUAL

CAPÍTULO II

GENERALIDADES DEL MANUAL

400 GLOSARIO

401 Usuario.- Cualquier persona militar o empleado civil permanente o temporal de la Armada del Ecuador.

402 Terceros.- Instituciones privadas o públicas que tengan relación con la Institución y Proveedores, todo el personal que pertenece a empresas que proveen productos o servicios a la Armada del Ecuador y personal temporal.

403 Jefe.- Instancia inmediata superior del personal militar o empleado civil que labora en el Armada del Ecuador.

404 Estándar.- Es una norma, regla, patrón o referencia que debe ser seguida por la audiencia para la que fue creada.

405 Confidencialidad.- Se refiere a que la información solo puede ser conocida por individuos autorizados.

406 Integridad.- Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc, por personas no autorizadas.

407 Disponibilidad.- Se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

408 Backup.- Consiste en realizar copias de seguridad de la información y hardware.

409 Estaciones de trabajo.- Es el computador asignado a un usuario de la Armada del Ecuador. Una estación de trabajo también se conoce como PC, equipo y máquina.

410 Identificación.- Es la identificación personal de ingreso a una aplicación tecnológica, identifica al usuario e ingresa a la aplicación con la clave de autenticación.

CAPÍTULO III

POLÍTICAS DE SEGURIDAD INFORMÁTICA

CAPÍTULO III

POLÍTICAS DE SEGURIDAD INFORMÁTICA

500 POLÍTICAS PARA EL CONTROL DE ACCESO DEL USUARIO

501 Registro de usuarios

Elaborar un procedimiento formal de registro de usuarios para otorgar acceso a los sistemas y servicios de información.

- Estandarizar en los Centros Tecnológicos de Información los parámetros almacenados en los perfiles de Usuarios.
- Requerir a los usuarios que firmen declaraciones indicando que entienden las condiciones de acceso al sistema.
- Eliminar inmediatamente los derechos de acceso de los usuarios que hayan cambiado de trabajo o hayan dejado la organización.
- Chequear de manera periódica, y eliminar los IDs de cuentas de usuario redundantes.
- Asegurar que no se emitan IDs de usuario redundantes a otros usuarios.
- Cuando el usuario deje de tener relación oficial con la Institución o la cuenta deje de ser utilizada por un tiempo definido más de 30 días, la cuenta deberá ser removida, para lo cual los jefes de personal de cada reparto deben notificar a los Centros Tecnológicos (Quito-Guayaquil) para el procedimiento respectivo.
- Cuando el usuario deje de laborar o de tener una relación con la Institución, el departamento de sistemas deberá ser notificado con un memorando u oficio a fin de que los administradores de sistemas procedan a tomar las medidas pertinentes con su información y cuenta de acceso.
- Los usuarios predeterminados por los sistemas operativos deben ser eliminados por el Administrador de Redes.

502 Permisos de usuarios

Restringir y controlar la asignación y uso de los privilegios a los usuarios, el uso inapropiado de los privilegios del sistema con frecuencia es un importante factor que contribuye a la falla de los sistemas que se han violado.

- El Administrador de Redes en el único encargado de la asignación de permisos a los usuarios.

- Identificar los privilegios asociados con el sistema, así como la asignación de los privilegios a las personas sobre una base "lo que necesitan saber" y "evento por evento"; es decir, el requerimiento mínimo para su rol funcional sólo cuando se necesita.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se debieran otorgar sino hasta que se complete el proceso de autorización.

503 Mantenimiento y Revisión de privilegios

Mantener un control efectivo sobre el acceso a los datos y servicios de información. Los Centros Tecnológicos deben realizar un proceso formal en intervalos regulares para revisar los derechos de acceso de los usuarios.

- Revisar los derechos de acceso de los usuarios a intervalos regulares (se recomienda un periodo de 6 meses).
- Revisar las autorizaciones para derechos de acceso privilegiados a intervalos más frecuentes (se recomienda un periodo de 3 meses).
- Chequear las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados.

504 Manejo de contraseñas del usuario

Las claves secretas son medios comunes para validar la identidad del usuario para tener acceso al sistema o servicio de información. La asignación de contraseñas secretas se debiera controlar a través de un proceso de gestión formal.

- Requerir a los usuarios que firmen una declaración para mantener confidenciales sus claves secretas personales y las contraseñas secretas del trabajo en grupo solamente dentro del grupo.
- Asegurar cuando se requiera a los usuarios que mantengan sus propias contraseñas secretas, que se les proporcione inicialmente una contraseña secreta temporal que están obligados a cambiar inmediatamente. Las claves secretas temporales provistas cuando los usuarios olvidan su contraseña secreta sólo se debieran suministrar después de una identificación positiva del usuario.
- Evitar que las contraseñas se guarden en el sistema de cómputo en una forma desprotegida.
- El acceso y custodia de todas las contraseñas de los usuarios es absoluta responsabilidad del administrador de la red siendo este el único responsable de su confidencialidad hasta la entrega al usuario final.

505 Uso de contraseñas por parte de los usuarios

La cooperación de los usuarios autorizados es esencial para una seguridad, los usuarios debieran estar concientes de sus responsabilidades para mantener controles de acceso efectivos particularmente con relación al uso de contraseñas secretas y la seguridad del equipo.

- Mantener sus contraseñas secretas en forma confidencial.
- Evitar mantener un registro escrito de sus contraseñas secretas, a no ser que se puedan guardar con seguridad.
- Cambiar su contraseña secreta cuando exista algún indicio de una posible violación en el sistema o contraseña secreta.
- Seleccionar contraseñas con un largo mínimo de seis a ocho caracteres que sean fáciles de recordar.
- Elaborar las contraseñas no basándose en algo que otra persona pueda adivinar fácilmente o que se puede obtener utilizando información relacionada con la persona, como nombres, número de teléfono, fechas de nacimiento, etc.
- Evitar que las contraseñas contengan caracteres idénticos consecutivos o grupos de sólo números o letras.
- Cambiar la contraseña por lo menos una vez cada 30 días usando las políticas de creación de contraseña.

Si los usuarios necesitan tener acceso a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se les debiera advertir que pueden utilizar una sola contraseña.

506 Equipos de usuario desatendido

Los usuarios debieran asegurarse que el equipo desatendido tenga la protección apropiada. El equipo instalado en áreas de usuarios como estaciones de trabajo o servidores de archivo, puede requerir protección específica del acceso no autorizado cuando se deja desatendido por un periodo extenso.

- Finalizar las sesiones activas cuando terminen, a no ser que puedan asegurarse mediante mecanismos de bloqueo apropiados como una pantalla asegurada mediante una clave secreta.
- Apagar las computadoras cuando acaban su trabajo.
- Asegurar las PCs o terminales del uso no autorizado mediante una tecla de bloqueo o un control equivalente (acceso con clave secreta).

600 POLÍTICAS PARA EL CONTROL DE ACCESO AL SISTEMA OPERATIVO

601 Identificación y autenticación del usuario

Todos los usuarios (incluyendo el personal de soporte técnico, como operadores, administradores de redes, programadores de sistemas y administradores de bases de datos) debieran tener un identificador único (ID del usuario) para su uso personal y singular de manera que las actividades pueden ser subsecuentemente monitoreadas a las personas responsables.

- Los IDs de ingreso a la red, los sistemas y los recursos informáticos tanto físicos como lógicos son propiedad de la Institución y se usarán exclusivamente para actividades relacionadas con ella.
- Ninguna ID de usuario podrá ser usada para propósitos ilegales, criminales o no éticos.

602 Inicio de sesión en un Terminal

El acceso a los servicios de información se debiera obtener vía un proceso de inicio de sesión seguro.

- No presentar los identificadores del sistema o la aplicación hasta que se haya completado exitosamente el proceso de inicio de sesión.
- Presentar una advertencia general que a esa computadora sólo tienen acceso los usuarios autorizados.
- Evitar la presentación de mensajes de asistencia que ayuden a un usuario no autorizado durante el procedimiento de inicio.
- Validar la información de inicio de sesión sólo después de haber llenado todos los datos. Si surge un error el sistema no debiera indicar qué datos son correctos o incorrectos.
- Limitar el número de intentos de inicios de sesión fallidos permitidos (tres intentos es lo recomendado).
    - registrar los intentos fallidos.
    - establecer un tiempo de espera antes de permitir más intentos de inicio o rechazar cualquier otro intento sin una autorización específica.
    - desconectar las conexiones de enlace.
- Presentar la siguiente información al completar un inicio de sesión exitoso:
    - fecha y hora del inicio exitoso anterior;
    - detalles de cualquier intento de inicio fallido desde el último inicio exitoso.

603 Terminales Inactivas

Las terminales inactivas debieran cerrarse después de un periodo definido de inactividad para evitar el acceso de personas no autorizadas, este medio de cierre debiera limpiar la pantalla del terminal y cerrar tanto las aplicaciones como las sesiones en red.

604 Monitoreo del acceso del sistema

Producir y mantener registros de auditoria que detallen las excepciones y otros eventos relevantes a la seguridad para un periodo acordado para ayudar al monitoreo del acceso del sistema, incluyendo:

- ID`s de los de usuario
- Fechas y horas de ingresos y salidas
- Identidad del terminal o locación si fuese posible
- Registros de intentos exitosos y rechazados de acceso al sistema
- Registros de intentos exitosos y rechazados de acceso a datos y otros recursos

605 Monitoreo del uso del sistema

Se deban establecer procedimientos para el monitoreo del uso de medios de procesamiento de información, asegurando que los usuarios sólo realicen actividades para las cuales han sido autorizados.

a. acceso autorizado, incluyendo:
    a. ID del usuario:
    b. fecha y hora de eventos claves (tipos de eventos)
    c. archivos a los cuales se tuvo acceso
    d. el programa/utilidades utilizados
b. intentos de accesos no autorizados, como:
    a. intentos fallidos
    b. violaciones de la política de acceso y los avisos para los portales y firewalls de la red
    c. alertas de los sistemas de detección de intrusión propios
c. alertas o fallas en el sistema, como:
    a. alertas o mensajes en la consola
    b. excepciones en el registro del sistema
    c. alarmas en el manejo de la red

El resultado de las actividades de monitoreo se debiera revisar regularmente, la frecuencia de la revisión dependerá de los riesgos involucrados. Se deberían incluir:

- el grado crítico de los procesos de aplicación
- el valor, sensibilidad y grado critico de la información involucrada
- la experiencia previa de infiltración y mal uso del sistema
- el grado de interconexión del sistema (particularmente con redes públicas).

700 POLÍTICAS DE CONTROL DE ACCESO A LA APLICACIÓN

701 Restricción al acceso a la información

Los usuarios de los sistemas de aplicación, incluyendo el personal de apoyo, debieran tener un acceso a las funciones de los sistemas de información y aplicación en concordancia con una política de control de acceso definida, basado en los requerimientos de la política de acceso a la información Institucional.

- Restringir el conocimiento de los usuarios sobre las funciones del sistema de información o aplicación para las cuales no tienen acceso autorizado con la edición apropiada de la documentación del usuario.
- Controlar los derechos de acceso de los usuarios (leer, escribir, eliminar y ejecutar).
- Asegurar que los datos de salida de los sistemas de aplicación que manejan información confidencial sólo contengan información relevante y sólo se envíe a terminales y locaciones autorizadas.

702 Sistema sensible o confidencial

Los sistemas sensibles o confidenciales deben requerir un ambiente de cómputo dedicado. Algunos sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial y requieren de un trato especial.

- Identificar la sensibilidad de un sistema de aplicación explícitamente por el propietario de la aplicación.

800 POLÍTICAS PARA EL MANEJO DE LA INFORMACIÓN

801 Educación y capacitación en seguridad de la información

Todos los empleados de la Institución y, cuando sea relevante, las terceras personas debieran recibir una capacitación apropiada y actualizaciones regulares sobre las políticas y procedimientos Institucionales. Esto incluye los requerimientos de seguridad, responsabilidades legales y controles, así como el uso correcto de los medios de procesamiento de la información, antes de concederles acceso a la información o servicios.

- Prohibir el almacenamiento de información clasificada como secretísima y secreta en las estaciones de trabajo, la misma que debe ser manejada de acuerdo al manual de administración de documentación de la Institución.
- Los usuarios deberán utilizar únicamente los servicios para los cuales están autorizadas. Los usuarios no pueden utilizar las cuentas de otras personas ni intentar de apoderarse de las claves de acceso, como tampoco intentar burlar los sistemas de seguridad bajo ningún punto de vista.
- Cada usuario de un Pc será responsable de mantener los debidos resguardos en cuanto a confidencialidad de los datos almacenados.

802 Medios de información y de procesamiento de información

La información y los medios de información debieran ser protegidos de una divulgación, modificación o robo por personas no autorizados, y se debieran establecer controles para minimizar la pérdida o daño.

- Almacenar adecuadamente en archivadores y/o otras formas de muebles seguros los medios en documentos y computadora cuando no están en uso, especialmente fuera de las horas de trabajo.
- Guardar la información confidencial o crítica en una caja fuerte o archivadora resistente al fuego cuando no se la requiera.
- Proteger los puntos de ingreso y salida de correo y las máquinas de fax desatendidos.
- Las fotocopiadoras debieran mantenerse aseguradas fuera de las horas de trabajo normales.
- La información confidencial o clasificada, cuando está impresa, debiera ser eliminada de las impresoras inmediatamente.

803 Backup de la Información

Generar copias de backup de la información y software esencial de manera regular.

- Mantener en un local remoto un nivel mínimo de información backup, junto con registros exactos y completos de las copias backup y los procedimientos de restauración documentados, a una distancia

suficiente para escapar a cualquier daño de un desastre en el departamento.

- Probar regularmente los medios de backup para asegurar que se pueda confiar en ellos para un uso de emergencia cuando sea necesario.
- Los respaldos serán de dos tipos, diario y semanal
- El respaldo diario se lo realizará al cierre de las operaciones
- El respaldo semanal se realizará el día viernes al cierre de las operaciones
- El respaldo debe ser realizado por el personal responsable del mismo

804 Mantenimiento de registro de actividades

El personal operacional debe mantener un registro de sus actividades en el sistema y registrar las fallas reportadas por los usuarios de los sistemas de procesamiento de la información y comunicaciones. Los registros deben incluir:

- momento de Inicio y fin de los sistemas.
- errores del sistema y las acciones correctivas tomadas.
- confirmación del manejo correcto de los archivos de datos y salidas de computación.
- el nombre de la persona que está realizando el ingreso en el registro.

Para el manejo de fallas deben incluir:

- revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente.
- revisión de las medidas correctivas para asegurar que los controles no se hayan comprometido y que la acción tomada esté completamente autorizada.

805 Documentación del sistema

La documentación del sistema puede contener un rango de información importante (descripciones de los procesos de aplicación, procedimientos, estructuras de datos, procesos de autorización).

- Almacenar de manera segura la documentación del sistema.
- Proteger apropiadamente la documentación del sistema que se mantiene en una red pública.

900 POLÍTICAS DE SEGURIDAD INSTITUCIONAL

901 Reuniones de la Directiva sobre seguridad de la información

La seguridad de la información es una responsabilidad compartida por todos los miembros de la directiva, por lo tanto, se debiera considerar un foro para asegurar que exista una dirección clara y un apoyo visible para las iniciativas de seguridad.

- Establecer los roles y responsabilidades específicos para la seguridad de la información en toda la organización.
- Establecer las metodologías y procesos específicos para la seguridad de la información (evaluación de riesgo, sistema de clasificación de seguridad).
- Establecer y respaldar las iniciativas de información a nivel de toda la organización (programa de conciencia de seguridad).
- Evaluar la idoneidad y coordinar la implementación de los controles específicos de seguridad de la información para sistemas o servicios nuevos.
- Revisiones de los incidentes de seguridad de la información.
- Promover la publicidad de las políticas de la Seguridad de la Información.
- El administrador de redes deberá realizar un informe por escrito de los empleados que infrinjan repetidamente las políticas de seguridad, siguiendo el órgano regula correspondiente, para que sean sancionados.
- Se debe tener los mismos tipos de Administradores (base de datos, aplicaciones, redes y comunicaciones) en ambos Centros Tecnológicos para el manejo de los sistemas Institucionales.
- La aplicación de políticas, normas, procedimientos y uso de aplicaciones para el control de Seguridad Informática debe ser estandarizada en ambos Centros Tecnológicos.

902 Clasificación de la Información

Asegurar que los activos de información reciban un nivel de protección apropiado, clasificada por necesidades, prioridades y grado de protección, verificando los varios grados de sensibilidad y criticidad.

903 Plan de Contingencias

- Elaborar un Plan de Contingencias en el cual especifique los procedimientos a seguir en caso de un desastre (antes, durante y después del desastre), con sus respectivos responsables del cumplimiento de los procedimientos.
- Revisar, actualizar y analizar el Plan de Contingencias de manera anual o según eventualidades ocurridas en la Institución.
- Realizar procedimientos de concientización sobre la importancia del Plan de Contingencias.

- Realizar charlas informativas al personal de los procedimientos existentes en el Plan de Contingencias, así como también realizar simulacros del mismo, para así recabar información para el mejoramiento del Plan.

1000 POLÍTICAS PARA MANEJO DE EQUIPOS

1001 Equipos Móviles

Cuando se utiliza medios de computación móvil, como notebooks, palms, laptops y teléfonos móviles, se debiera tener cuidado de asegurar que no se comprometa la información.

- Incluir los requerimientos de protección física, controles de acceso, técnicas de criptografía, backups y protección contra virus.
- Mantener actualizados los procedimientos contra el software malicioso.
- Asegurar el equipo que contiene información importante, sensible y/o crítica bajo llave o algún tipo de seguro.
- Establecer la capacitación para el personal que usa computación móvil para elevar su conocimiento sobre los riesgos adicionales resultantes.

1002 Lista de activos

Elaborar una lista de activos de la Institución para conocer la importancia, valor, niveles de protección, y ubicación del activo. Se debe incluir como activo a:

- a los activos de información bases de datos y archivos de datos, documentación, manual del usuario, material de capacitación, procedimientos operacionales y de apoyo, planes de continuidad, acuerdos de reserva, información archivada.
- activos de software: software de aplicación, software del sistema, herramientas y servicios de desarrollo
- activos físicos equipo de cómputo (procesadores, rnonitores, laptops, módems, etc.), equipo de comunicación (routers, switches, cableado, maquinas contestadotas, etc.), medios magnético (cintas y discos), otro equipo técnico (suministros de energía, unidades de aire acondicionado), muebles, ambientes.
- servicios de computación y servicios de comunicaciones, servicios generales, como: calefacción, iluminación, energía, aire acondicionado.

1003 Mantenimiento de equipo

El equipo debiera ser mantenido correctamente para asegurar la disponibilidad e integridad continua.

- Mantener el equipo en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor.
- Realizar las reparaciones y servicio al equipo con el personal de mantenimiento de hardware del Centro Tecnológico.
- Mantener registros de todas las fallas sospechadas o reales y de todo el mantenimiento preventivo y correctivo.
- Mantener los controles apropiados cuando se envía equipo fuera del departamento para mantenimiento.

- Prohibir a los usuarios abrir las máquinas, hacer cambios no autorizados en el hardware, sea cambios de memorias, discos y mas partes constitutivas del equipo.
- La división de mantenimiento deberá elaborar un cuadro de mantenimiento preventivo trimestral o semestral de acuerdo a la disponibilidad de tiempo y personal.
- Restringir el cambio de configuración de los equipos que se ha sido determinado por el CETEIN respectivo.
- Estandarizar las configuraciones de las estaciones de trabajo administradas por ambos Centros Tecnológicos.
- Realizar un inventario de equipos con los respectivos números de serie (teclado, mouse, monitor, CPU),modelo, software instalado y responsable del equipo. Es importante que se verifique con el usuario la constancia del inventario realizado, así como la firma de las dos partes.

1004 Ubicación y protección del equipo

El equipo debiera ser ubicado o protegido de manera que se reduzcan los riesgos de los peligros ambientales y las oportunidades para un acceso no autorizado.

- Monitorear las condiciones ambientales para detectar condiciones que podrían afectar adversamente a la operación de los medios de procesamiento de la información.
- Considerar el impacto de un desastre que ocurra cerca al departamento por ejemplo, un incendio en un edificio vecino, filtración de agua del techo o pisos por debajo del nivel del suelo.
- Ubicar los equipos de manera que se minimice el acceso innecesario a las áreas de trabajo.
- Prohibir comer, beber y fumar en las cercanías a los medios de procesamiento de la información.

1005 Equipos y dispositivos

- Todo equipo computacional y de comunicación de datos pertenecientes a la Armada deberán permanecer en el lugar asignado por los Centros Tecnológicos, adicionalmente restringir la conexión de dispositivos a las PCs que no sean suministradas por los Centros Tecnológicos y en el caso de necesitarlo se debe solicitar la autorización respectiva.
- Estandarizar en ambos Centros Tecnológicos los servidores de Dominio, Base de datos, Aplicaciones, Proxy. Mail, Firewall, así como los sistemas operativos y aplicaciones para el desarrollo Institucional.
- Disponer de servidores de backup en caso de una emergencia para así tener el menor impacto dentro de la Institución.

1006 Suministros de energía

El equipo debiera ser protegido de fallas de energía, y otras anomalías eléctricas, se debiera proporcionar un suministro eléctrico adecuado que satisfaga las especificaciones de la red.

- Incluir múltiples alimentadores para evitar un solo punto de falla en el suministro de energía.
- Utilizar un suministro de energía sin interrupciones (UPS), realizando su chequeo regularmente para asegurar que tiene la capacidad adecuada.
- Utilizar un generador de reserva para que el procesamiento continúe en caso de una falla de energía prolongada.
- Aplicar la protección contra rayos (pararrayos) en todos los edificios.

1007 Cableado

El cableado de energía y telecomunicaciones que lleva datos o sostiene los servicios de información se debieran proteger de la interceptación o daño.

- Implementar líneas de energía y telecomunicaciones subterráneas, para el ingreso a los medios de procesamiento de información.
- Proteger el cableado de la red de una interceptación no autorizada o daño, utilizando conductos porta cables o al evitar las rutas a través de áreas públicas.
- Separar los cables de energía de los cables de comunicaciones para evitar la interferencia.
- Para los sistemas sensibles o críticos los controles adicionales a considerarse incluyen:
    - la instalación de conductos porta cables blindados y habitaciones o cajas cerradas en los puntos de inspección y terminación
    - uso de rutas o medios de transmisión alternativos
    - uso de cableado de fibra óptica

1008 Mantenimiento del Centro Cómputo

Al interior del Centro de Cómputo se deberá tener las condiciones apropiadas de, temperatura 10° a 15° C y humedad (aire acondicionado), piso antiestático y se deberá contar con protección contra incendios tanto los detectores de humo como los extintores, así como su respectivo mantenimiento periódico.

1009 Manejo de los medios computarizados removibles

Realizar procedimientos para el manejo de los medios computarizados removibles (cintas, discos, casetes y reportes impresos).

- Borrar los contenidos previos de cualquier medio re-usable que va a ser retirado de la Institución.
- Realizar un registro de todos los medios retirados de la Institución previa su autorización.
- Almacenar en un ambiente seguro los medios de almacenamiento.

1010 Eliminación de los medios

Cuando ya no se requieran los medios debieran ser eliminados de una manera segura, la información confidencial puede filtrarse a personas externas a través de una eliminación negligente de los medios.

- Almacenar y eliminar de una manera segura (incineración o trituración) los medios que contienen información sensible (cintas, disquetes, grabaciones de voz, documentación en papel).

2000 POLÍTICAS PARA EL ACCESO FÍSICO

2001 Barreras Físicas

La protección física se puede lograr creando varias barreras físicas (una pared, control mediante tarjetas o una recepcionista) alrededor del departamento y los medios de procesamiento de la información.

- Implementar mecanismos de control (alarmas, seguros) en el área que albergue los medios de procesamiento de información.
- Establecer un área de recepción con personal u otros medios de control de acceso físico al departamento o edificio.

2002 Controles de ingreso físico

Se debieran proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que sólo se permita el ingreso del personal autorizado.

- Registrar fecha y hora de ingreso de los visitantes que van a las áreas seguras.
- Controlar el acceso a la información sensible y los medios de procesamiento de información sólo las personas autorizadas. Utilizando controles de autenticación, como: lectora de tarjetas para autorizar y validar todo acceso.
- Requerir que todo el personal use alguna forma de identificación visible y se debiera fomentar que cuestionen a las personas extrañas o cualquier que no esté utilizando la identificación visible.

2003 Asegurar oficinas, salas y medios

La selección y diseño de un área segura debiera tomar en cuenta la posibilidad de daño por incendio, inundación, explosión y otras formas de desastre natural.

- Dar la mínima indicación del propósito de los departamentos, evitando signos obvios dentro o fuera que identifiquen la presencia de actividades de procesamiento de la información.
- Situar las funciones y equipos de apoyo (fotocopiadoras, fax) dentro del área segura para evitar las demandas de acceso, que podrían comprometer la información.
- Colocar sistemas adecuados para la detección de intrusos instalados de acuerdo a estándares profesionales y se debieran probar regularmente para cubrir todas las puertas externas y ventanas accesibles.
- Separar los medios de procesamiento de información manejados por la Institución de terceras personas.
- Situar el equipo de reserva y medios de backup a una distancia prudencial para evitar el daño en caso de desastre en el área de equipos.

2004 Contratos con terceras personas

Los acuerdos que involucran el acceso de terceras personas a los medios de procesamiento de información Institucional se debieran basar en un contrato formal conteniendo, o refiriéndose a, todos los requerimientos de seguridad para asegurar la conformidad con las políticas y estándares de seguridad de la organización. El contrato debe contener:

- La política general sobre la seguridad de la información
- Protección de activos, incluyendo
    a. procedimientos para proteger los activos Institucionales, incluyendo la información y hardware.
    b. procedimientos para determinar si algo ha puesto en peligro los activos (pérdida o modificación de los datos).
    c. controles para asegurar la devolución o destrucción de la información y activos al final de, o en un punto acordado en el tiempo durante el contrato.
    d. integridad y disponibilidad.
    e. restricciones sobre la copia y divulgación de información.
- Provisión para la transferencia de personal cuando sea apropiado.
- Las respectivas obligaciones de las partes durante el contrato.
- Las responsabilidades con respecto a temas legales.
- Acuerdos de control de acceso:
- métodos de acceso permitido, y el control y uso de identificadores singulares como IDs y claves secretas de usuarios,
    a. un proceso de autorización para el acceso y privilegios de los usuarios.
    b. un requerimiento para mantener una lista de las personas autorizadas a los servicios disponibles y sobre cuáles son sus derechos y privilegios con respecto a dicho uso.
- La identificación de criterios de desempeño verificables, su monitoreo y reporte;
- El establecimiento de un proceso de intensificación para la solución de problemas; cuando sea apropiado se deberían considerar acuerdos para contingencias
- Responsabilidades relacionadas con la instalación y mantenimiento de hardware
- Una clara estructura de reporte y formatos de reporte establecidos
- Un proceso claro y especificado para la gestión de cambio.
- Capacitación del usuario y el administrador en los métodos, procedimientos y seguridad
- Controles para asegurar la protección contra el software malicioso
- Acuerdos para el reporte, notificación e investigación de incidentes de seguridad y violaciones en la seguridad.

2005 Sistemas de oficina electrónicos

Los Sistemas de oficina electrónicos proporcionan oportunidades para una difusión e intercambio más rápido de la información comercial utilizando una combinación de documentos computadoras computación móvil, comunicaciones móviles correo de voz, comunicaciones de voz en general,

multimedia, servició medios postales y máquinas de fax, es por esto que se debe preparar e implementar políticas y lineamientos para controlar los riesgos comerciales y de seguridad.

- Controlar las vulnerabilidades de la información en los sistemas de oficina (grabación de las llamadas telefónicas o conferencias telefónicas, confidencialidad de las llamadas, archivo de faxes)
- Controlar el manejo del intercambio de información (el uso de boletines electrónicos corporativos)
- Restringir el acceso a la información diaria relacionada con personas seleccionadas (personal que trabaja en proyectos confidenciales).
- Restringir los medios seleccionados a categorías de usuarios específicos.
- Retención y backup de la información mantenida en el sistema.

3000 POLÍTICAS PARA EL MANEJO DE LA INFORMACIÓN

3001 Debilidades en la seguridad

Requerir que los usuarios de los servicios de información noten y reporten cualquier debilidad de seguridad observada o sospechada, o las amenazas, en los sistemas o servicios, indicando a su jefe inmediato.

3002 Mal funcionamiento del software

Establecer los procedimientos para reportar cualquier mal funcionamiento en el software. Considerando las siguientes acciones:

- Anotar los síntomas del problema y cualquier mensaje que aparezca en la pantalla.
- Detener el uso de la computadora. Si se va a examinar el equipo, debiera ser desconectado de las redes Institucionales antes de volverlo a encender. Los disquetes no debieran ser transferidos a otras computadoras.
- Reportar inmediatamente el problema al encargado de la seguridad de la información.
- Prohibir a los usuarios que no eliminen el software en sospecha a no ser que se le autorice a eso. El personal apropiadamente capacitado y experimentado debiera llevar a cabo la recuperación.

3003 Instalación de aplicaciones

- Las licencias de todo el software que usa la COGMAR deberán ser entregadas al Centro Tecnológico el que será el encargado de la administración y custodia de las mismas.
- La instalación del software y parches está a cargo de la división de mantenimiento de los Centros Tecnológicos, ellos serán los únicos autorizados a instalar software en las diferentes estaciones de trabajo de la COGMAR a mas de los administradores de red, adicionalmente se restringe al usuario el acceso al disco donde reside el sistema operativo.
- Queda prohibido instalar copias de software pirata, puesto que además de transgredir la ley de propiedad intelectual, marcas y patentes, pueden contener virus, spyware (software que espía la máquina atacada), archivos de sistema incompatibles con los del usuario, lo cual puede provocar su inestabilidad y fallas en el equipo.
- Actualizar los Sistemas Operativos Windows 9x de las estaciones de trabajo por razones de seguridad.

3004 Compartir carpetas y archivos

Uno de los métodos mas difundidos por los últimos ataques de virus es el de infectar las máquinas replicándose a si mismos en las carpetas compartidas, dentro de una red. Por lo que los usuarios deben tomar las medidas siguientes:

- Si un usuario debe compartir una carpeta con otro o varios usuarios, esa carpeta debe tener una clave de acceso, la misma que deberá ser cambiada periódicamente. Especificando que usuarios comparte la misma.
- Luego de que no se requiera más el compartir el recurso en cuestión debe deshabilitarse la opción de compartir dicha carpeta.

3005 Desarrollo de Aplicaciones

- En el proceso de desarrollo de las aplicaciones se debe seguir una metodología y métricas estándar de desarrollo aprobada y analizada de acuerdo a los requerimientos de la Institución.
- Verificar la consistencia de los datos utilizados por las aplicaciones generadas realizando pruebas, antes de su implementación.
- Implementar controles dentro del desarrollo de aplicaciones para evitar la fuga o robo de información.
- Realizar la documentación de la aplicación (fecha de implementación, analista y programador responsable, objetivos, diagramas de flujo, archivos de entrada- salida que se utiliza y el manual de usuario) para posteriores análisis, cambios o mantenimiento del mismo.
- En el caso de que existiera la participación de terceros en el desarrollo de la aplicación el código fuente como la información utilizada para el mismo debe regirse a las norma impuestas por la Institución.

4000 POLÍTICAS PARA CONTROL DE ACCESO A LA RED

4001 Uso de los servicios de la red

Las conexiones inseguras a los servicios en red pueden afectar a toda la Institución, sólo se debiera proporcionar a los usuarios acceso directo a los servicios que se le ha autorizados utilizar específicamente.

- Realizar procedimientos de autorización para determinar quién está autorizado a tener acceso a qué redes y servicios en red.

4002 Terminal de usuario al servicio de cómputo

La ruta desde la terminal del usuario al servicio de cómputo necesita ser controlada para evitar el acceso y uso no autorizado de los medios de información. Podemos reducir dichos riesgos incorporando controles que restringen la ruta entre la terminal del usuario y los servicios de cómputo a los cuales el usuario está autorizado a ingresar.

- Asignar líneas o número telefónicos dedicados.
- Evitar el recorrido ilimitado en la red.
- Hacer cumplir el uso de sistemas de aplicación y/o puertas de seguridad especificados para los usuarios de redes externas.
- Controlar activamente las comunicaciones fuente a destino permitido vía seguridad.
- Restringir el acceso a la red estableciendo dominios lógicos separados, como redes privadas virtuales para grupos de usuarios dentro de la Institución.

4003 Segregación en redes

Segregar la red principal en dominios de red lógicos separados por los dominios internos de la Institución y los dominios de red externos, cada uno protegido por un perímetro de seguridad definido (firewalls físicos y lógicos) tomando en cuenta la visión de crecimiento de la red y a la vez separados por servicios de información y usuarios.

4004 Control de conexión en red

- Realizar controles de acceso para redes compartidas restringiendo la capacidad de conexión de los usuarios, en aplicaciones como:
  - correo electrónico
  - transferencia de archivos en un solo sentido
  - transferencia de archivos en ambos sentidos
  - acceso interactivo
  - acceso a la red vinculado a la hora del día o fecha.
- Identificar los puntos físicos de voz y datos, comprobar su validez y etiquetarlos para el control y mantenimiento de los puntos de red.
- Realizar pruebas periódicas de los puertos de red para verificar si permanecen habilitados o no de acuerdo a las normas establecidas.
- Realizar un análisis para la implementación de un canal de backup de las diferentes redes en caso de emergencia.

5000 POLÍTICAS DE ACCESO AL INTERNET

5001 Uso del Internet

- El servicio de internet de la COGMAR está dirigido a ciertos usuarios de la red que por su cargo o función necesitan de este servicio y comprende indistintamente tanto a los señores oficiales, tripulantes o empleados civiles.
- Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.
- Habilitar el uso del Chat externo a usuarios autorizados.
- No contestar los mensajes SPAM, ya que al hacerlo se re-configurará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.
- Borre constantemente los cookies, archivos temporales e historial del internet, con la opción Herramientas, Opciones de Internet, de su navegador.

5002 Software Malicioso

La protección contra software malicioso se debiera basar en la conciencia de seguridad, acceso apropiado al sistema mediante controles de detección y prevención.

- Indicar medidas de protección de los riesgos asociados al obtener archivos y software, ya sea desde o vía redes externas.
- Instalar y actualizar software anti-virus y de reparación para analizar las computadoras y medios, ya sea como un control de precaución o de manera rutinaria.
- Realizar revisiones regulares del software y el contenido de los datos de los sistemas que sostienen los procesos críticos.
- Chequear antes de usar cualquier archivo en los medios electrónicos de origen incierto o no autorizado o los archivos recibidos a través de redes no confiables, para verificar si tienen virus.
- Chequear antes de usar cualquier archivo adjunto en el correo electrónico y las descargas para ver si tienen algún software malicioso.
- Realizar procedimientos para lidiar con la protección contra virus en los sistemas (recuperación de ataques de virus).
- En caso de recibir un mensaje bajo sospecha de virus, debe contactarse con su área de soporte técnico o con el administrador de la red.

5003 Antivirus

- EL administrador del antivirus debe configurar al antivirus corporativo para rastrear toda la red permanentemente. El la configuración deben constar el rastreo de los discos duros de las máquinas, los disquetes, los archivos de correo adjunto, archivos descargados de la web, etc.

- Realizar el monitoreo diario de los servidores y estaciones de trabajo, los usuarios y las versiones de software antivirus instalado en cada uno de ellos para actualizar el antivirus a los equipos que no se encuentren con el software actualizado o detectar posibles infecciones y acciones inmediatas a tomar.

5004 Correo Electrónico

La Institución debe controlar en el uso del correo electrónico:

- ataques por correo electrónico (virus, intercepción).
- protección de los archivos adjuntos del correo electrónico.
- responsabilidad del empleado de no comprometer a la Institución (enviando un correo electrónico difamatorio, utilizándolo para hostigamiento, compras no autorizadas).
- uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (firmas digitales).
- retención de mensajes que, si se guardan pueden ser descubiertos en caso de litigio.
- controles adicionales para analizar los mensajes que no pueden ser autenticados.
- No descargar archivos con extensión .exe, .vbs, avi, protectores de pantalla, etc. que no provengan de un usuario conocido. En estos casos, se les recomienda borrar inmediatamente el mensaje sin abrirlo y de ser detectados por el administrador serán borrados desde el servidor.

Biografía

MÓNICA ALEXANDRA LLERENA FUENMAYOR

DATOS PERSONALES

Fecha y lugar de nacimiento: Quito, 03 de Diciembre de 1982

Cédula de Identidad: 171782383-3

EDUCACIÓN

Primaria:

- Unidad Educativa Naval (Liceo Naval) – Quito
- Colegio Nuestra Madre de la Merced – Guayaquil

Secundaria:

- Colegio Nuestra Madre de la Merced -Guayaquil
- Unidad Educativa Naval (Liceo Naval) – Quito

Superior:

- Escuela Politécnica del Ejército, Sangolquí. Facultad de Ingeniería en Sistemas e Informática

OTROS

- Escuela Politécnica Del Ejército / Instituto de Idiomas – Diploma de Suficiencia en el Idioma Inglés (25/04/2003)
- Participación "I Seminario de Inteligencia Artificial NeuroESPE-2004" (04/02/04)
- Participación en el " I Congreso Nacional de Redes de Comunicaciones ESPENET 2003" (04/02/04)
- Minicurso "Implementación de Redes Inalámbricas" – I Congreso Nacional de Redes de Comunicación ESPEnet 2003 (21/07/03)

JOSÉ DAVID SAÁ CHONLONG

DATOS PERSONALES

Fecha y lugar de nacimiento: Quito, 10 de Agosto de 1982

Cédula de Identidad: 171401883-3

EDUCACIÓN

Primaria:

- Cardenal Spellman (4to Escolta de Honor del Estandarte del Plantel)

Secundaria:

- Colegio Militar Eloy Alfaro

Superior:

- Escuela Politécnica del Ejército, Sangolquí. Facultad de Ingeniería en Sistemas e Informática

OTROS

- Escuela Politécnica Del Ejército / Instituto de Idiomas – Diploma de Suficiencia en el Idioma Inglés (11/10/2004)
- Minicurso "Detección y Solución de Problemas en REDES LAN" realizado en el "I Congreso Nacional de Redes de Comunicaciones ESPENET 2003. (04/02/04)
- Participación en el " I Congreso Nacional de Redes de Comunicaciones ESPENET 2003" (04/02/04)
- Participación en el " I Seminario de Inteligencia Artificial NeuroEspe-2004" (21/07/03)
- MCP en Desarrollo de Páginas Web en C#.Net (17/09/2005)
- Certificación CISCO CCNA1 Networking Basics (06/09/2004)

HOJA DE LEGALIZACION DE FIRMAS

ELABORADA(O) POR

Mónica Alexandra Llerena Fuenmayor

José David Saá Chonlong

DECANO DE LA FACULTAD DE INGENIERIA SISTEMAS E INFORMÁTICA

_____

Sr. TCRN. EM

Ing. Marco Quintana

Decano

Sangolquí, 20 de Abril de 2006